(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年2 月13 日 (13.02.2003)

PCT

(10) 国際公開番号
WO 03/013068 A1

(51) 国際特許分類[7]: H04L 12/28

(21) 国際出願番号: PCT/JP02/07714

(22) 国際出願日: 2002 年7 月30 日 (30.07.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-229078 2001 年7 月30 日 (30.07.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 川村 晴美 (KAWAMURA,Harumi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 嶋 久登 (SHIMA,Hisato) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 山田 英治, 外(YAMADA,Eiji et al.); 〒104-0041 東京都 中央区 新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

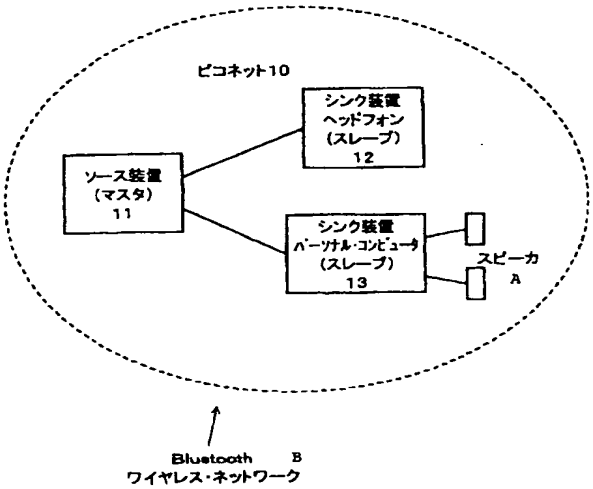
(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

[続葉有]

(54) Title: RADIO COMMUNICATION SYSTEM, RADIO COMMUNICATION CONTROL APPARATUS, RADIO COMMUNICATION CONTROL METHOD, RECORDING MEDIUM, AND COMPUTER PROGRAM

(54) 発明の名称: 無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラム



10...PICO NET
11...SOURCE DEVICE (MASTER)
12...SINK DEVICE HEADPHONE (SLAVE)
13...SINK DEVICE PERSONAL COMPUTER (SLAVE)
A...LOUDSPEAKER
B...BLUETOOTH WIRELESS NETWORK

(57) Abstract: When transmitting data to be protected such as audio data by Bluetooth connection, authentication difficulty is switched according to the processing ability of the device to be a communication mate. Accordingly, even a device having a low processing ability can perform Bluetooth communication based on SDMI. Moreover, when the communication mate is a device having a high processing ability such as a personal computer, it is possible to provide sufficient countermeasure for hacking.

[続葉有]

WO 03/013068 A1

添付公開書類:
— 国際調査報告書

(57) 要約:

オーディオ・データなどプロテクションを施す必要があるデータをＢｌｕｅｔｏｏｔｈ接続により伝送する場合、通信相手となる機器の処理能力に応じて認証の難易度を切り替える。したがって、低い処理能力の機器であっても、ＳＤＭＩに準拠したＢｌｕｅｔｏｏｔｈ通信を行うことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、充分なハッキング対策を施すことができる。

明 細 書

無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラム

[技術分野]

本発明は、複数の機器間をワイヤレスで接続するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに係り、特に、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを伝送するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに関する。

さらに詳しくは、本発明は、Ｂｌｕｅｔｏｏｔｈのように１台のマスタ（ｍａｓｔｅｒ）機器と複数台のスレーブ（ｓｌａｖｅ）機器によって構成されるピコネット（ｐｉｃｏｎｅｔ）内において機器間でオーディオ・データを伝送するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに係り、特に、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらＢｌｕｅｔｏｏｔｈ機器間で伝送する無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに関する。

[背景技術]

最近、デジタルＶＴＲやＭＤ（ミニディスク（商標））記録再生装置などのデジタル記録装置が普及し始めている。さらに、記録機能を備えたＤＶＤ（デジタルビデオディスク（商標）あるいはデジタル・バーサタイル・ディスク）装置も登場し、パーソナル・コンピュータ（ＰＣ）などの機器に搭載されるようになってきている。

このようなデジタル情報記録装置によれば、デジタル形式のデータやコンテン

ツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の複製に関する法規制を強化するだけでは不充分であり、情報技術の観点からもデータやコンテンツの正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると思料される。

例えば、デジタル音楽の著作権保護を目的として、１９９８年に米国大手レコード会社などが中心となってＳＤＭＩ（Secure Digital Music Interactive）なるフォーラムが設立された。ＳＤＭＩでは、基本的には、何らプロテクションが掛けられていない状態でデジタル形式のコンテンツを機器外に出力することを禁止している。したがって、オーディオ再生機器からスピーカやヘッドフォンなどのレンダリング（Rendering）装置にコンテンツをデジタル出力する場合、あるいは、ＤＶＤ－Ｒドライブやパーソナル・コンピュータ（ＰＣ）などのレコーディング（Recording）装置にコンテンツをデジタル出力する場合などにおいて、伝送されるデータ・コンテンツをプロテクトすることが必須（すなわち、"unprotected digital out"の禁止）とされている。

例えば、ＳＤＭＩでは、ポータブル音楽プレーヤで著作権を保護する仕組みとして"Ｓｃｒｅｅｎｉｎｇ"という機能が規定されている。Ｓｃｒｅｅｎｉｎｇとは、ポータブル・デバイス（ＰＤ）のメモリ・レコーダ上にコピーしてよいコンテンツか否かを検査する仕組みであり、電子透かしを利用することが既に合意されている。例えば、不正に配信されたコンテンツや、既に１回（若しくは許容回数だけ）コピーされたコンテンツからはもはやコピーできないように、電子透かしによってＳｃｒｅｅｎｉｎｇをかけることができる。

このようなＳＤＭＩの要請は、ポータブル機器間をケーブル接続する場合は勿論のこと、ワイヤレスで機器間接続する場合においても必須とされている。

ところで、最近では、近距離無線通信の代表例である"Ｂｌｕｅｔｏｏｔｈ"が、普及し始めて、各種の情報機器に搭載されている。Ｂｌｕｅｔｏｏｔｈは、さまざまな業界に対して適用可能なワイヤレス接続インターフェースを提供する標準規格であり、"Ｂｌｕｅｔｏｏｔｈ　ＳＩＧ（Special Interest Group）"にその運営や管理などが委ねられている。

Ｂｌｕｅｔｏｏｔｈは、２．４ＧＨｚのＩＳＭ（Industry Science Medical）バンドと呼ばれるグローバルな無線周波数を使用し、全体のデータ伝送速度は１Ｍｂｐｓであり、その中には電話の音声伝送に利用可能な６４ｋｂｐｓの同期伝送チャンネルと、データ伝送のための非同期伝送チャンネルが設けられている。前者の同期伝送チャンネルは、ＳＣＯ（Synchronous Connection Oriented Link）伝送方式が採用され、回線接続に適用される。また、後者の非同期伝送チャンネルは、ＡＣＬ（Asynchronous Connection Less Link）伝送方式が採用され、パケット交換によるデータ伝送に適用される。Ｂｌｕｅｔｏｏｔｈによる機器間の接続範囲は１０ｍ程度であるが、追加増幅器を使用することによって、さらに１００ｍまで延長することができる。

Ｂｌｕｅｔｏｏｔｈの技術仕様は、「コア（Ｃｏｒｅ）」と「プロファイル（Ｐｒｏｆｉｌｅ）」に大別される。コアは、Ｂｌｕｅｔｏｏｔｈが提供するワイヤレス接続の基礎を定義する。これに対し、プロファイルは、Ｂｌｕｅｔｏｏｔｈのコアに基づいて各種の機能やアプリケーションを開発して機器に組み込む際に、機器間の相互接続性を保証するための各機能毎に規定された技術要件の集まりである。

Ｂｌｕｅｔｏｏｔｈのプロファイルは複数存在し、その組み合わせにより１つのアプリケーション（「利用モデル（Ｕｓａｇｅ）」とも呼ぶ）を提供する。実際には、アプリケーションを提供するプロファイルの組み合わせがコアとともにＢｌｕｅｔｏｏｔｈ製品に実装されることになる。

例えば、携帯電話やパーソナル・コンピュータ関連のプロファイルを始めとして、自動車、ネットワーク、プリンタ、オーディオ、ビデオなど、さまざまなＢｌｕｅｔｏｏｔｈプロファイルが想定される。

例えば、オーディオ・データの伝送用のプロファイルとして、"Bluetooth Advanced Audio Distribution Protocol"（Ａ２ＤＰ）を挙げることができる。このプロファイルによれば、ＡＶ再生機器とスピーカやヘッドフォンなどのレンダリング装置とのワイヤレス接続や、ＡＶ再生機器とのＤＶＤ－Ｒドライブやパーソナル・コンピュータ（ＰＣ）などのレコーディング装置とのワイヤレス接続を実現することができる。

この種のＢｌｕｅｔｏｏｔｈ搭載のＡＶ機器においても、先述したＳＤＭＩに準拠するためには、"unprotected digital out"を禁止するための仕組み、すなわち、デジタル伝送されるオーディオ・データをプロテクトするための仕組みを装備する必要がある。

Ｂｌｕｅｔｏｏｔｈセキュリティは、ある特定の２端末間で「リンク・キー（Ｌｉｎｋ　Ｋｅｙ）」と呼ばれる共通のパラメータを設定することを基本として、マスタと各スレーブ間で１対１のセキュリティが管理される（リンク・キーは第３者には開示されない）。

ここで、デジタル・データをプロテクトする要素としては、「盗み取り（盗み聴き）」対策のための暗号化（encryption）と、「なりすまし」対策のための認証（authentication）という２つに大別される。

Ｂｌｕｅｔｏｏｔｈ　ＳＩＧでは、コンテンツのプロテクション方式に関しては関与していないため、各ベンダの責任でコンテンツのプロテクションを行わなければならない。しかしながら、Ｂｌｕｅｔｏｏｔｈ搭載のオーディオ機器間での認証方式は、Ｂｌｕｅｔｏｏｔｈ層ではなく、その上位のアプリケーション層で実装しなければならない。

本発明者等は、Ｂｌｕｅｔｏｏｔｈ通信をヘッドフォンやスピーカなどのレンダリング（すなわち聴くだけ）の用途に使用する場合と、レコーディングの用途に使用する場合とでは、プロテクションの仕組みが異なるものと思料する。

レコーディングに関しては、Ｍｕｓｉｃ　Ｄｏｗｎｌｏａｄの場合のように、アプリケーション毎に充分納得のいく高い強度レベルのプロテクションが採用される場合が多い。

これに対し、レンダリングに関しては、どの程度の強度とするかまで規定しているケースは少ない。例えば、ヘッドフォンのように処理能力の低いＣＰＵが搭載されている機器に対して高いレベルのプロテクションを要求又は必須とすることは困難である。

例えば、ｉ－ＬＩＮＫ（ＩＥＥＥ　１３９４）用のコピー・プロテクション規格であるＤＴＣＰ（Digital Transmission Content Protection）の Full authentication を適用するためには、ＭＩＰＳ　Ｒ４０００　１００ＭＨｚのＣ

ＰＵで計算しておおよそ６００ｍｓの演算時間を要する負荷となる。このようなＣＰＵのコストや処理時間をヘッドフォンのような末端のポータブル機器に課すことは現実的ではない。また、バッテリ駆動を基本とするポータブル機器においては、システム・デザイン上で消費電力が大きな問題となり、このような過大なレベルの認証方式を一律に採用することは困難である。

一方において、レコーディング機能を装備したパーソナル・コンピュータ（ＰＣ）がレンダリング用途であると偽って不正に記録することを防止しなければならない。

ヘッドフォンのような演算能力が低い機器に対して採用し易いように、レンダリング用途として、例えば８ビットのキーを用いた認証方式を採用した場合、演算能力が高いパーソナル・コンピュータから簡単に破られてしまい、プロテクションを行う意味が薄れてしまう。

[発明の開示]

本発明の目的は、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

本発明のさらなる目的は、Ｂｌｕｅｔｏｏｔｈのように１台のマスタ（ｍａｓｔｅｒ）機器と複数台のスレーブ（ｓｌａｖｅ）機器によって構成されるピコネット（ｐｉｃｏｎｅｔ）内において機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

本発明のさらなる目的は、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらＢｌｕｅｔｏｏｔｈ機器間で伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、所定の無線セル内でデータ・ストリームを送信するＳｏｕｒｃｅ装置とデータ・ストリームを受信するＳｉｎｋ装置とからなる無線通信システムであって、

前記Ｓｉｎｋ装置の処理能力を判別する判別手段と、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御手段と、

を具備することを特徴とする無線通信システムである。

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

また、前記無線セルは、例えばＢｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築される「ピコネット」である。ピコネット内では、通信秩序を維持する１台のマスタ装置が複数台のスレーブ装置と１対１のＢｌｕｅｔｏｏｔｈ通信を行なうことができる。

前記判別手段は、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプの装置か、又は、処理能力の高い第２のタイプの装置かを判別する。また、前記認証制御手段は、前記Ｓｉｎｋ装置が第１のタイプの場合は比較的簡単な認証方式を採用し、前記Ｓｉｎｋ装置が第２のタイプの場合は比較的複雑な認証方式を採用する。

本発明の第１の側面に係る無線通信システムによれば、オーディオ・データなどプロテクションを施す必要があるデータをＢｌｕｅｔｏｏｔｈ接続により伝送する場合、通信相手となる機器の処理能力に応じて認証方式の難易度を切り替えることで、適切なコンテンツ・プロテクションを行なうことができる。したがって、ヘッドフォンのようなレンダリング機能しか持たない低い処理能力の機器であっても、ＳＤＭＩに準拠したＢｌｕｅｔｏｏｔｈ通信を行なうことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、充分なハッキング対策を施すことができる。

前記判別手段は、前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義される

Stream Get Capability コマンドを用いて前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別することができる。

また、前記判別手段は、例えば、ＡＶＤＴＰプロトコルで定義されるSecurity Control コマンドを用いて前記Ｓｉｎｋ装置に処理能力を問い合わせることができる。

また、前記判別手段は、前記Ｓｉｎｋ装置の種別を基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、問い合わせ（Ｉｎｑｕｉｒｙ）処理手続の際に入手したClass of Device情報を基に、前記Ｓｉｎｋ装置の処理能力を判別することができる。

また、前記判別手段は、前記Ｓｉｎｋ装置がサポートするサービスを基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、サービス・ディスカバリ（Service Discovery）によって取得された前記Ｓｉｎｋ装置が対応するサービス（プロトコル又はプロファイル）によってその処理能力を判別することができる。

例えば、前記判別手段は、前記Ｓｉｎｋ装置がＡ２ＤＰ（Bluetooth Advanced Audio Distribution Profile）にのみ対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプであると判断することができる。

あるいは、前記判別手段は、前記Ｓｉｎｋ装置がＰＡＮ(Personal Area Network)、ＬＡＮ（LAN Access Profile)、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのうち少なくとも１つのプロファイルに対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプではないと判断することができる。

また、本発明の第２の側面は、所定の無線セル内でＳｉｎｋ装置に対してデータ・ストリームを送信する無線通信制御装置又は無線通信制御方法であって、

前記Ｓｉｎｋ装置の処理能力を判別する判別手段又はステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御手段又はステップと、

を具備することを特徴とする無線通信制御装置又は無線通信制御方法である。

前記無線セルは、例えばＢｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより

構築される「ピコネット」である。ピコネット内では、通信秩序を維持する１台のマスタ装置が複数台のスレーブ装置と１対１のＢｌｕｅｔｏｏｔｈ通信を行うことができる。また、本発明の第２の側面に係る無線通信制御装置又は無線通信制御方法を、Ｂｌｕｅｔｏｏｔｈピコネット内のマスタ装置に実装することができる。

前記判別手段又はステップは、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプの装置か、又は、処理能力の高い第２のタイプの装置かを判別する。また、前記認証制御手段は、前記Ｓｉｎｋ装置が第１のタイプの場合は比較的簡単な認証方式を採用し、前記Ｓｉｎｋ装置が第２のタイプの場合は比較的複雑な認証方式を採用する。

本発明の第２の側面に係る無線通信制御装置又は無線通信制御方法によれば、オーディオ・データなどプロテクションを施す必要があるデータをＢｌｕｅｔｏｏｔｈ接続により伝送する場合、通信相手となる機器の処理能力に応じて認証方式の難易度を切り替えることで、適切なコンテンツ・プロテクションを行なうことができる。したがって、ヘッドフォンのようなレンダリング機能しか持たない低い処理能力の機器であっても、ＳＤＭＩに準拠したＢｌｕｅｔｏｏｔｈ通信を行なうことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、充分なハッキング対策を施すことができる。

前記判別手段又はステップは、前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、オーディオ伝送用のＡＶＤＴＰプロトコルで定義されるStream Get Capabilityコマンドを用いて前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別することができる。

また、前記判別手段又はステップは、例えば、ＡＶＤＴＰプロトコルで定義されるSecurity Controlコマンドを用いて前記Ｓｉｎｋ装置に処理能力を問い合わせることができる。

また、前記判別手段又はステップは、前記Ｓｉｎｋ装置の種別を基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、問い合わせ（Ｉｎｑｕｉｒｙ）処理手続の際に入手したClass of Device情報を基に、前記Ｓｉｎｋ

装置の処理能力を判別することができる。

また、前記判別手段又はステップは、前記Ｓｉｎｋ装置がサポートするサービスを基に前記Ｓｉｎｋ装置の処理能力を判別するようにしてもよい。例えば、サービス・ディスカバリによって取得された前記Ｓｉｎｋ装置が対応するサービスによってその処理能力を判別することができる。

例えば、前記判別手段又はステップは、前記Ｓｉｎｋ装置がＡ２ＤＰにのみ対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプであると判断することができる。

あるいは、前記判別手段又はステップは、前記Ｓｉｎｋ装置がＰＡＮ、ＬＡＮ、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのうち少なくとも１つのプロファイルに対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプではないと判断することができる。

また、本発明の第３の側面は、所定の無線セル内でＳｉｎｋ装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記Ｓｉｎｋ装置の処理能力を判別する判別ステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とする記憶媒体である。

本発明の第３の側面に係る記憶媒体は、例えば、様々なプログラム･コードを実行可能な汎用コンピュータ･システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Flexible Disk）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第３の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る無線通信システム、あるいは第２の側面に係る無線通信制御装置及び無線通信制御方法と同様の作用効果を得ることができる。

また、本発明の第４の側面は、所定の無線セル内でＳｉｎｋ装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・プログラムであって、

前記Ｓｉｎｋ装置の処理能力を判別する判別ステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とするコンピュータ・プログラムである。

本発明の第４の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第４の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る無線通信システム、あるいは第２の側面に係る無線通信制御装置及び無線通信制御方法と同様の作用効果を得ることができる。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

[図面の簡単な説明]

図１は、本発明の一実施形態に係るＢｌｕｅｔｏｏｔｈピコネット１０内の構成を模式的に示した図である。

図２は、図１に示したＢｌｕｅｔｏｏｔｈピコネット１０を構成するＳｏｕｒｃｅ装置としてのオーディオ・プレーヤ（マスタ）１１と、Ｓｉｎｋ装置としてのヘッドフォン（スレーブ）１２の構成を模式的に示した図である。

図３は、オーディオ伝送用のプロファイル" Bluetooth Advanced Audio Distribution Profile "（Ａ２ＤＰ）のプロファイル・スタック構造を模式的に示した図である。

図４は、ＡＶＤＴＰプロトコルにおける接続確立手続（Connection Establishment）のシーケンスを示した図である。

図５は、ＡＶＤＴＰプロトコルで定義されているＳｅｃｕｒｉｔｙ Ｃｏｎｔｒｏｌ手続のシーケンスを示した図である。

図６は、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにおけるオーディオ・ストリーミングの流れとパケット・フォーマットを模式的に示した図である。

図７は、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２間でのＧＡＶＤＰに従ってストリーミングのセットアップと解放を行うためのＳｏｕｒｃｅ装置とＳｉｎｋ装置間での処理の流れを示した図である。

図８は、ＡＶＤＴＰプロトコルで定義されている認証手続きに成功した場合にシーケンスを示した図である。

図９は、ＡＶＤＴＰプロトコルで定義されている認証手続きに失敗した場合にシーケンスを示した図である。

図１０は、本実施形態に係るＢｌｕｅｔｏｏｔｈピコネット１０において、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２間で行われる認証の処理手順の概念を示したブロック図である。

図１１は、"Stream Get Capability"のコマンドに使用されるデータ・フレームの構造を示した図である。

図１２は、"Stream Get Capability"コマンドに対するレスポンスに使用されるデータ・フレームの構造を示した図である。

図１３は、"Stream Set Configuration"のコマンド及びレスポンスに使用され

るデータ・フレームの構造を示した図である。

図１４は、"Security Control"コマンドに使用されるデータ・フレームの構造を示した図である。

図１５は、"Security Control"コマンドに対するレスポンスに使用されるデータ・フレームの構造を示した図である。

図１６は、タイプ問い合わせ時の"Security Control"コマンドの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図１７は、タイプ問い合わせ時の"Security Control"コマンドに対するレスポンスの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図１８は、Ｃｌａｓｓ　ｏｆ　Ｄｅｖｉｃｅ情報フィールドのデータ構造を模式的に示した図である。

図１９は、Bluetooth Assigned Numbers が規定する Major Device Class の割り当てを示した図である。

図２０は、認証時の"Security Control"コマンドの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図２１は、認証時の"Security Control"コマンドに対するレスポンスの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図２２は、Ｓｏｕｒｃｅ装置がＳｉｎｋ装置のタイプ判別を行うことにより認証を行うための処理手順（前半）を示したフローチャートである。

図２３は、Ｓｏｕｒｃｅ装置がＳｉｎｋ装置のタイプ判別を行うことにより認証を行うための処理手順（後半）を示したフローチャートである。

図２４は、ＵＵＩＤの例（抜粋）を示した図である。

[発明を実施するための最良の形態]

以下、図面を参照しながら本発明の実施形態について詳解する。

本発明に係る認証方式によれば、認証に成功した場合に限り通信相手はレンダ

リング用途でストリームを受ける機器であるとみなすことができる。この結果、伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

以下、Ｂｌｕｅｔｏｏｔｈでオーディオ伝送を行う場合を例にとって、図面を参照しながら本発明の実施形態について詳解する。

Ｂｌｕｅｔｏｏｔｈは、２．４ＧＨｚのＩＳＭ（Industry Science Medical）バンドと呼ばれるグローバルな無線周波数を使用し、全体のデータ伝送速度は１Ｍｂｐｓであり、その中には電話の音声伝送に利用可能な６４ｋｂｐｓの同期伝送チャンネルと、データ伝送のための非同期伝送チャンネルが設けられている。前者の同期伝送チャンネルは、ＳＣＯ（Synchronous Connection Oriented Link）伝送方式が採用され、回線接続に適用される。また、後者の非同期伝送チャンネルは、ＡＣＬ（Asynchronous Connection Less Link）伝送方式が採用され、パケット交換によるデータ伝送に適用される。

Ｂｌｕｅｔｏｏｔｈの技術仕様は、「コア（Ｃｏｒｅ）」と「プロファイル（Ｐｒｏｆｉｌｅ）」に大別される。コアは、Ｂｌｕｅｔｏｏｔｈが提供するワイヤレス接続の基礎を定義する。これに対し、プロファイルは、Ｂｌｕｅｔｏｏｔｈのコアに基づいて各種の機能やアプリケーションを開発して機器に組み込む際に、機器間の相互接続性を保証するための各機能毎に規定された技術要件の集まりである。Ｂｌｕｅｔｏｏｔｈのプロファイルは複数存在し、その組み合わせにより１つのアプリケーション（「利用モデル（Ｕｓａｇｅ）」とも呼ぶ）を提供する。実際には、アプリケーションを提供するプロファイルの組み合わせがコアとともにＢｌｕｅｔｏｏｔｈ製品に実装されることになる。

Ｂｌｕｅｔｏｏｔｈは、１対１のケーブル代替接続だけではなく、１対多の簡易ワイヤレス・ネットワークの構築も提供する。このため、Ｂｌｕｅｔｏｏｔｈ通信に関わる機器群の中の１つに制御機能を与えることで通信の秩序を保つようにしている。制御機能を与えられた機器のことを「マスタ（Ｍａｓｔｅｒ）」機器と呼び、それ以外を「スレーブ（Ｓｌａｖｅ）」機器と呼ぶ。また、マスタ及びスレーブとなった機器群が通信状態にあるネットワークのことを「ピコネット（ｐｉｃｏｎｅｔ）」と呼ぶ。

ピコネット内では、「ピコネット内同期」がとられており、通信状態にあるすべてのＢｌｕｅｔｏｏｔｈ機器は、マスタ機器を基準とした同一の周波数ホッピング・パターンと時間スロットを有している状態にある。時間スロットはマスタ機器が提供するＢｌｕｅｔｏｏｔｈクロックを基準として各スレーブ機器が形成する。

ピコネット内には、必ず１つだけマスタ機器が存在し、このマスタ機器が１台以上のスレーブを制御しながら通信を行なう。また、ピコネット内では、すべてのパケットはマスタ機器とスレーブ機器の間でのみ受信され、スレーブ機器どうしが直接通信を行なうことはできない。

そして、１つのピコネット内で同じ通信できるスレーブは最大７台までと決められている。これらにマスタ機器を含めて、最大で８台のＢｌｕｅｔｏｏｔｈ機器がピコネット内で同時通信を行なうことができる。

ここで、オーディオ・ビジュアル（ＡＶ）機器の分野において、Ｂｌｕｅｔｏｏｔｈ通信を導入した場合、ステレオ・コンポやメディア・プレイヤなどのオーディオ・データ・ストリームの出力源となるＳｏｕｒｃｅ装置１１をマスタとして定義する一方で、ヘッドフォンやパーソナル・コンピュータ（ＰＣ）などのオーディオ出力ターゲットとなるＳｉｎｋ装置をスレーブ機器として定義することができる。図１には、このように構成されたＢｌｕｅｔｏｏｔｈピコネット１０内の構成を模式的に示している。

［従来の技術］の欄でも既に述べたように、このようにオーディオ伝送に適用されたＢｌｕｅｔｏｏｔｈワイヤレス・ネットワークがＳＤＭＩ(Secure Digital Music Interactive)に準拠するためには、Ｓｏｕｒｃｅ装置１１からＳｉｎｋ装置１２へ向かう伝送路に対して、"unprotected digital out"を禁止するための仕組み、すなわち、デジタル伝送されるオーディオ･データをプロテクトするための仕組みを装備する必要がある。

デジタル･データをプロテクトする要素としては、「盗み取り（盗み聴き）」対策のための暗号化（encryption）と、「なりすまし」対策のための認証(authentication)の２つに大別される。

本実施形態に係るＢｌｕｅｔｏｏｔｈワイヤレス・ネットワークでは、前者の

暗号化に関しては、Ｂｌｅｔｏｏｔｈ層で定義された暗号化方式をそのまま適用するので、本明細書では詳細な説明を省略する。

また、後者の認証方式に関しては、Ｂｌｕｅｔｏｏｔｈ層ではなく、その上位のアプリケーション層で実装する。本実施形態に係る認証方式は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受ける機器であるとみなして、伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データをプロテクトするが、その詳細な説明は後述に譲る。

図２には、図１に示したＢｌｕｅｔｏｏｔｈピコネット１０を構成するＳｏｕｒｃｅ装置としてのオーディオ・プレーヤ（マスタ）１１と、Ｓｉｎｋ装置としてのヘッドフォン（スレーブ）１２の構成を模式的に示している。

Ｓｏｕｒｃｅ装置としてのオーディオ・プレーヤ１１は、Ｂｌｕｅｔｏｏｔｈインターフェース・ブロック１１Ａと、信号生成ブロック１１Ｂと、プレーヤ制御ブロック１１Ｃと、システム制御ブロック１１Ｄとで構成され、Ｂｌｕｅｔｏｏｔｈピコネット１０内ではマスターとして機能する。

Ｂｌｕｅｔｏｏｔｈインターフェース・ブロック１１Ａは、ピコネット１０内におけるＢｌｕｅｔｏｏｔｈワイヤレス接続を実現するための機能ブロックであり、ピコネット１０内におけるスレーブ機器１２，１３との制御信号の交換やオーディオ・データの伝送などを行う。

信号生成ブロック１１Ｂは、オーディオ信号を生成するための機能ブロックである。

プレーヤ制御ブロック１１Ｃは、オーディオ・プレーヤ１１上におけるメディアの再生、停止、一時停止、早送り、巻き戻しなどのメディア再生制御機能を実現するための機能ブロックである。

システム制御ブロック１１Ｄは、Ｂｌｕｅｔｏｏｔｈピコネット１０内における各スレーブ機器１２，１３の統合的な制御を実現するための機能ブロックである。本実施形態では、システム制御ブロック１１Ｄは、ＡＶ機器間のオーディオ・データの伝送用のプロファイルである"Advanced Audio Distribution Profile"（Ａ２ＤＰ）におけるＳｏｕｒｃｅの機能を管理するようになっている。

Ａ２ＤＰプロファイルは、Ｂｌｕｅｔｏｏｔｈピコネット１０内でのオーディオ伝送のプロテクトも規定している。Ｂｌｕｅｔｏｏｔｈセキュリティは、ある特定の２端末間で「リンク・キー（Ｌｉｎｋ　Ｋｅｙ）」と呼ばれる共通のパラメータを設定することを基本として、マスタと各スレーブ間で１対１のセキュリティが管理される（リンク・キーは第３者には開示されない）。

オーディオ・データをプロテクトする要素としては、「盗み取り（盗み聴き）」対策のための暗号化（encryption）と、「なりすまし」対策のための認証（authentication）という２つに大別される。本実施形態では、暗号化に関しては、Ｂｌｕｅｔｏｏｔｈ層で定義されている暗号化方式を使用する。また、認証方式に関しては、Ａ２ＤＰプロファイルでは規定されていないので、上位のアプリケーション層（後述）において、本発明に固有の認証方式を実装する。本発明に係る認証方式によれば、Ｓｏｕｒｃｅ装置１１は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受けるＳｉｎｋ機器であるとみなすことができる。この結果、Ｓｏｕｒｃｅ装置側では、Ｓｉｎｋ装置において伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

ヘッドフォン１２は、Ｂｌｕｅｔｏｏｔｈインターフェース・ブロック１２Ａと、ヘッドフォン制御ブロック１２Ｂと、信号処理ブロック１２Ｃとで構成される、レンダリング専用のＳｉｎｋ装置である。

Ｂｌｕｅｔｏｏｔｈインターフェース・ブロック１２Ａは、Ｂｌｕｅｔｏｏｔｈピコネット１０内におけるＢｌｕｅｔｏｏｔｈワイヤレス接続を実現するための機能ブロックであり、マスタ装置としてのオーディオ・プレーヤ１１との制御信号の交換、並びにオーディオ・データの受信などを行う。

ヘッドフォン制御ブロック１２Ｂは、ボリューム・アップ、ボリューム・ダウン、ミュートなどヘッドフォン１２による音声出力機能を実現するための機能ブロックである。

信号処理ブロック１２Ｃは、Ｂｌｕｅｔｏｏｔｈワイヤレス通信によりマスター装置１１から受信されたオーディオ信号を処理する機能ブロックである。

本実施形態では、ヘッドフォン１２は、従来のオーディオ伝送用のプロファイ

ル" Bluetooth Advanced Audio Distribution Profile "（Ａ２ＤＰ）に対応した従来と同様のスレーブ装置として構成することができる。

図３には、オーディオ伝送用のプロファイル"Bluetooth Advanced Audio Distribution Profile "（Ａ２ＤＰ）のプロファイル・スタック構造を模式的に図解している。

同図において、ベースバンド層、ＬＭＰ層、Ｌ２ＣＡＰ層、ＳＤＰ層、及び、ＡＶＤＴＰ層の各層は、Ｂｌｕｅｔｏｏｔｈコアで定義されたＢｌｕｅｔｏｏｔｈプロトコルである。このうちベースバンド層、ＬＭＰ層、Ｌ２ＣＡＰ層は、ＯＳＩ（Open Systems Interconnect：開放型システム間相互接続）基本参照モデルの第１層及び第２層に相当する。

ＳＤＰ層は、Ｂｌｕｅｔｏｏｔｈサービス・ディスカバリ・プロトコル(Service Discovery Protocol）を規定するプロトコル層である。システム・コントローラとしてのマスタ装置１１は、このＳＤＰプロトコルを用いて、同じＢｌｕｅｔｏｏｔｈピコネット１０内のスレーブ機器１２，１３が備える機能又はサービスを検出することができる。

ＡＶＤＴＰ（Audio/Video Distribution Transport Protocol）層は、Ｂｌｕｅｔｏｏｔｈピコネット１０内におけるオーディオ伝送の処理手順やメッセージ交換を規定するプロトコル層であり、データ・ストリームのパラメータのネゴシエーションを行うシグナリング・エンティティと、データ・ストリーム自体を取り扱うトランスポート・エンティティとからなる。

Ａ２ＤＰでは、Ｂｌｕｅｔｏｏｔｈベースバンド層での暗号化をオプショナルとして実装することが可能である。Ａ２ＤＰでは、プロテクションに関して規定はしない。暗号化方式及び認証方式に関しては、Ａ２ＤＰの各プロテクション方式毎に定める。

アプリケーション層は、Ｓｏｕｒｃｅ装置１１又はＳｉｎｋ装置１２においてアプリケーション・サービスやトランスポート・サービスの各パラメータを設定するエンティティで構成される。アプリケーション層は、オーディオ・ストリーム・データを規定のパケット・フォーマットに適合させる処理も行なう。

本実施形態では、アプリケーション層は、Ｂｌｕｅｔｏｏｔｈピコネット１０

内におけるオーディオ伝送のための認証方式も実装する。この認証方式によれば、Ｓｏｕｒｃｅ装置１１は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受けるＳｉｎｋ機器であるとみなすことができる。この結果、Ｓｏｕｒｃｅ装置１１は、Ｓｉｎｋ装置側で伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

図３に示したプロファイル・スタック上では、Ｂｌｕｅｔｏｏｔｈピコネット１０内のＳｏｕｒｃｅ装置１１とＳｉｎｋ装置１２，１３間でのオーディオ伝送における設定、制御、操作を行なうことができる。但し、このプロファイル・スタックでは、１対多のデータ配信を行なうことはできない。

また、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２，１３間でのオーディオ伝送には、無線信号処理や、データ・ストリームのバッファリングや符号化／復号化のためにある程度の遅延が存在する。

また、このプロファイル・スタックを実装するためには、オーディオ・データの伝送レートは、Ｂｌｕｅｔｏｏｔｈリンク上で使用可能なビット・レートよりも充分小さくなければならない。これは、聴覚可能なノイズや音飛びの原因となるパケット消失の影響をなくすためのパケット再伝送を行なうためである。

Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにおけるオーディオ伝送を行うためのプロトコルであるＡＶＤＴＰは、「シグナリング」と「ストリーミング」という２つの機能に大別される。

ストリーミングは、オーディオ信号をリアルタイム伝送することを規定する。また、シグナリングは、Ｓｏｕｒｃｅ装置から送信されたオーディオ・ストリームをＳｉｎｋ装置側で受信処理できるように、フォーマットなどのネゴシエーションを行う。このネゴシエーション・パラメータの１つとして、コンテンツ・プロテクション（Content Protection：ＣＰ）のタイプがある。

Ｂｌｕｅｔｏｏｔｈ　ＡＶ伝送に適用するプロテクション方式はあらかじめＢｌｕｅｔｏｏｔｈ　ＳＩＧに登録しておき、Ｂｌｕｅｔｏｏｔｈ　ＳＩＧ側では各プロテクション方式に対して識別情報（ＩＤ）を割り振る。このＩＤについては、”Ｂｌｕｅｔｏｏｔｈ　Ａｓｓｉｇｎｅｄ　Ｎｕｍｂｅｒｓ”で参照すること

ができる。勿論、登録されたプロテクション方式の内容については、Ｂｌｕｅｔｏｏｔｈの仕様書には何ら記述されない。例えば、本発明に係るコンテンツ・プロテクション方式も、Ｂｌｕｅｔｏｏｔｈ ＳＩＧの管轄外でライセンスすることにより、規制を設けることもできる。

ＡＶＤＴＰプロトコルでは、接続確立手続（Connection Establishment）において、"Stream Get Capability"コマンドを用いて、Ｓｏｕｒｃｅ装置はオーディオ伝送先となるＳｉｎｋ装置が対応しているプロテクション方式を調べる。また、Ｓｏｕｒｃｅ装置は、"Stream Set Configuration"コマンドによりＩＤを指定することにより、適用するプロテクション方式をＳｉｎｋ装置に設定する（ＡＶＤＴＰプロトコルでは、コンテンツのプロテクション方式のＩＤは、Bluetooth Assigned Numbersに登録されるので、一義に決まる）。

図４には、ＡＶＤＴＰプロトコルにおける接続確立手続（Connection Establishment）のシーケンスを示している。ＡＶＤＴＰプロトコルではＢｌｕｅｔｏｏｔｈデバイスのＳｔｒｅａｍ入出力口としてＳｔｒｅａｍ Ｅｎｄ Ｐｏｉｎｔを規定している。Ｓｏｕｒｃｅ装置は、"Stream End Point Discovery"コマンドを用いて、Ｓｉｎｋ装置が何系統のストリームに対応しているか、及び、それぞれに対応しているストリーム・タイプ（オーディオかビデオか）について調べる。次いで、Ｓｏｕｒｃｅ装置は、"Stream Get Capability"を用いて、オーディオ伝送先となるＳｉｎｋ装置が対応しているプロテクション方式を調べる。その後、ＳＯｕｒｃｅ装置がＯｐｅｎコマンドをＳｉｎｋ装置に送ることにより、Ｓｏｕｒｃｅ装置とＳｉｎｋ装置はともに「オープン」状態になる。

Ｂｌｕｅｔｏｏｔｈオーディオ伝送において適用するプロテクション方式に応じてその後の処理方法は異なるが、本実施形態では、アプリケーション層において、ＡＶＤＴＰプロトコルで定義されている"Security Control"コマンドを用いてＳｉｎｋ装置の認証を行なうことによってプロテクションを行なう("Security Control"コマンドのパラメータは、各プロテクション方式毎に定義することができる)。

図５には、ＡＶＤＴＰプロトコルで定義されているＳｅｃｕｒｉｔｙ Ｃｏｎｔｒｏｌ手続のシーケンスを示している。図示の通り、オープン状態又はストリ

ーミング状態で"Security Control"コマンドの処理が行なわれる。この処理によってＢｌｕｅｔｏｏｔｈ伝送のステートの変化は生じない。

本実施形態では、Ｓｏｕｒｃｅ装置１１は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受けるＳｉｎｋ機器であるとみなすことによって、Ｓｉｎｋ装置において伝送データのレンダリングのみが行なわれる（言い換えれば、レコーディングは行なわれない）ことを想定したオーディオ伝送を行なうが、その詳細については後述に譲る。

ストリーミングに関しては、オーディオ伝送のためのプロファイルである"Advanced Audio Distribution Profile"（Ａ２ＤＰ）に記されている。図６には、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにおけるオーディオ・ストリーミングの流れとパケット・フォーマットを模式的に示している。

オーディオ・コンテンツのストリーミングを開始したいときには、まず、ストリーミング・コネクションのセットアップを行う。このセットアップ処理手続の間、各装置間でオーディオ・ストリーミングのための適切なパラメータを選択する。アプリケーション・サービス・ケイパビリティと、トランスポート・サービス・ケイパビリティという２種類のサービスが構成される。Ａ２ＤＰプロファイルでは、シグナリング処理手続に必要なオーディオ仕様パラメータを規定している。

Ａ２ＤＰのアプリケーション・サービス・ケイパビリティは、オーディオＣＯＤＥＣケイパビリティとコンテンツ・プロテクション・ケイパビリティとで構成される。

また、トランスポート・サービス・ケイパビリティは、ストリーミング・パケットを好適に取り扱うことができるように、ＡＶＤＴＰプロトコルで提供されているサービスを選択する。

ストリーミング接続が確立すると、ストリーミング開始処理手続が実行される。ＡＶＤＴＰプロトコルを用いてストリーミング伝送を行なう際の処理手続については、"Generic Audio/Video Distribution Profile"（ＧＡＶＤＰ）で規定されている。

Ｓｏｕｒｃｅ装置とＳｉｎｋ装置はともに「ストリーミング状態」になり、オ

ーディオ・ストリームの送受信を即座に行なうことができる。Ｓｏｕｒｃｅ装置は"Send Audio Stream"処理手続を用いてオーディオ・データの送信を行ない、これに対し、Ｓｉｎｋ装置は"Receive Audio Stream"処理手続を用いてオーディオ・データの受信を行なう。

「オープン状態」にあるときに、Ｓｏｕｒｃｅ装置又はＳｉｎｋ装置がオーディオ・ストリームの送受信を開始したいときには、ＧＡＶＤＰで定義されているストリーミング開始（Start Streaming）処理手続を開始しなければならない。

"Send Audio Stream"処理手続では、Ｓｏｕｒｃｅ装置は、シグナリング・セッションで、伝送データを選択されたフォーマットに符号化する。Ｓｏｕｒｃｅ装置のアプリケーション層では、符号化データを定義されたメディア・ペイロード（ＭＰ）フォーマットに適合させる。コンテンツ・プロテクション（ＣＰ）を利用する場合には、コンテンツ・プロテクション方式に依存したＣＰヘッダを、暗号化されたオーディオ・コンテンツの先頭に付加する。

その後、ストリーム・データは、インターフェース経由でＡＶＤＴＰ層で処理され、ＡＶＤＴＰプロトコルで定義されるトランスポート・サービスを用いて、トランスポート・チャンネルから送出される。

一方、Ｓｉｎｋ装置側のＡＶＤＴＰ層は、ＡＶＤＴＰプロトコルで定義されるトランスポート・サービスを用いて、トランスポート・チャンネルから受信して、インターフェース経由でアプリケーション層に受信ストリームを渡す。

コンテンツ・プロテクション方式が作動している場合、Ｓｉｎｋ装置側のアプリケーション層は、ＣＰヘッダの解析や暗号化コンテンツの解読を行なう。そして、オーディオ・データ・フレームは、所定のコーディング方式により復号化されて、オーディオ出力（レンダリング）などに利用される。

図７には、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２間でのＧＡＶＤＰに従ってストリーミングのセットアップと解放を行うためのＳｏｕｒｃｅ装置とＳｉｎｋ装置間での処理の流れを詳細に示している。但し、同図中で"＊"が付されたものは"Generic Access Profile"（ＧＡＰ）で規定されている処理手続であり、また、"＊＊"が付されたものは"Service Discovery Protocol"（ＳＤＰ）で定義されている処理手続であると理解されたい。ＧＡＰ及びＳＤＰは、Ｂｌｕｅｔｏｏ

ｔｈの共通基本機能である。

まず、Ｂｌｕｅｔｏｏｔｈピコネット１０内のマスタでもあるＳｏｕｒｃｅ装置１１は、該ピコネット１０内にどのようなスレーブが存在するかを調べるために、Ｉｎｑｕｉｒｙ（問合せ）を行なうためのＩＱパケットをピコネット１０内でブロードキャストする。

Ｉｎｑｕｉｒｙを受信したスレーブとしてのＳｉｎｋ装置１２は、自身のＢｌｕｅｔｏｏｔｈアドレス（BD_ADDR）やクロックの情報、機種の属性（Class of Device）を通知するためのＦＨＳパケットを返信する。

Ｓｏｕｒｃｅ装置１１は、ピコネット内の各スレーブから受信したＦＨＳパケットのデータを基に、どのスレーブと接続するかを選択する。ここでは、説明の便宜上、Ｓｉｎｋ装置１２を選択したものとする。

Ｎａｍｅ　Ｄｉｓｃｏｖｅｒｙ処理手続では、マスタとしてのＳｏｕｒｃｅ装置１１は、Ｐａｇｅ（呼び出し送信）により、スレーブとしてのＳｉｎｋ装置１２に宛てて、マスタの属性を通知して、マスタ及びスレーブ間で１対１の処理を経て通信フェーズに遷移する。そして、Ｎａｍｅ　Ｒｅｑｕｅｓｔにより、接続相手のＢｌｕｅｔｏｏｔｈ　Ｄｅｖｉｃｅ　Ｎａｍｅを取得する。

次いで、リンク確立（Link Establishment）処理手続では、ＢｌｕｅｔｏｏｔｈデバイスとしてのＳｏｕｒｃｅ装置１１とＳｉｎｋ装置１２間の物理リンクを構築する。このリンク確立処理手続の中には、Ｂｌｕｅｔｏｏｔｈベースバンド層（図３を参照のこと）における認証（Authentication）や暗号化のネゴシエーションも含まれる。但し、Ｂｌｕｅｔｏｏｔｈセキュリティは誤接続防止、盗聴防止を目的としているので、本発明に係る認証方式とは相違する、という点を充分理解されたい。

次いで、サービス・ディスカバリ（Service Discovery）、すなわち、スレーブが備える機能又はサービスを検出するために、ＳＤＰ用のＬ２ＣＡＰチャンネル（論理リンク・チャンネル）を張り、ＳＤＰプロトコルによりＳｉｎｋ装置１２がどのようなサービスに対応しているか（すなわち、Ｓｉｎｋ装置１２が対応しているプロトコル、プロファイルなどの情報）を知る。

そして、ＳＤＰ用のＬ２ＣＡＰチャンネルを解放してから、ＡＶＤＴＰシグナ

リングのためのＬ２ＣＡＰチャンネルを張る。既に述べたように、接続確立（Connection Establishment）処理手続の中で、オーディオＣＯＤＥＣ、サンプリング周波数などの情報を基に、コンテンツ・プロテクション方式に関する情報の開示及び設定が行なわれる。

本実施形態では、Ｓｏｕｒｃｅ装置１１は、ＡＶＤＴＰプロトコルにおける接続確立手続（Connection Establishment）において（図４を参照のこと）、"Stream Set Configuration"コマンドによりＩＤを指定することにより、適用するプロテクション方式をＳｉｎｋ装置１２に設定する。また、ＡＶＤＴＰプロトコルで定義されている"Security Control"コマンドを用いて（図５を参照のこと）、Ｓｉｎｋ装置１２のタイプ（すなわち、レンダリング用途でストリームを受ける機器であるか、又は、レコーディング用途でストリームを受ける機器か）を認証する。ヘッドフォンであるＳｉｎｋ装置１２は自分自身がレンダリング用途の機器であることを提示することによって、Ｓｏｕｒｃｅ装置１１側では、Ｓｉｎｋ装置１２においてレンダリング用途で伝送データ・ストリームを受けることを想定した認証方式が採用される。

認証に成功して、Ｓｉｎｋ装置１２がレンダリング用途の機器であることが明らかになった場合には、ＧＡＶＤＰで定義されているストリーミング開始（Start Streaming）処理手続を経て、オーディオ・ストリームの伝送が行なわれる。図８には、認証に成功したときのシーケンスを示している。同図に示すように、オープン状態において、Ｓｏｕｒｃｅ装置は、内部イベントの発生に応答して"Security Control"コマンドを発行して認証を行ない、これに成功すると、内部的なストリーミングの開始に応じて"Start Streaming"コマンドを発行して、Ｓｉｎｋ装置へのストリーミング伝送を行なう。

一方、認証に失敗した場合には、Ｓｏｕｒｃｅ装置１１側ではアプリケーション層に通知され、オーディオ・ストリームの伝送は行なわれない。図９には、認証に失敗したときのシーケンスを示している。同図に示すように、オープン状態において、Ｓｏｕｒｃｅ装置は、内部イベントの発生に応答して"Security Control"コマンドを発行して認証を行ない、これに失敗すると内部的な接続解放に応答して、"Connection Release"コマンドを発行してＳｉｎｋ装置との接続を

切断して、アイドル状態に遷移する。

図１０には、本実施形態に係るＢｌｕｅｔｏｏｔｈピコネット１０において、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２間で行われる認証の処理手順の概念を図解している。

Ｓｏｕｒｃｅ装置１１で発生した乱数ｘは、制御信号の一種としてＳｉｎｋ装置１２に伝送される。同図に示す例では、Ｓｏｕｒｃｅ装置１１とＳｉｎｋ装置１２はともに、ｆ（ｘ）で示される認証アルゴリズムを共有しており、Ｓｉｎｋ装置１２は受け取った入力ｘに対して演算を実行して、その演算結果ｆ’（ｘ）をＳｏｕｒｃｅ装置１１に制御信号の一種として送信する。そして、Ｓｏｕｒｃｅ装置１１は、乱数ｘから自分自身で算出した結果ｆ（ｘ）とＳｉｎｋ装置１２から受信した演算結果ｆ’（ｘ）とを比較して、これらが一致するか否かで認証の判断を行なう。

本実施形態に係る認証方式の特徴は、Ｓｏｕｒｃｅ装置１１は、認証の対象とするＳｉｎｋ装置１２のタイプによって演算方式ｆ（ｘ）を切り替えるという点にある。ここで言うＳｉｎｋ装置のタイプは、該装置がヘッドフォンなどの処理能力の低い機器か（Ｔｙｐｅ１）、又は、パーソナル・コンピュータ（ＰＣ）などの処理能力の高い機器か（Ｔｙｐｅ２）で区分される。

例えば、通信相手となるＳｉｎｋ装置がヘッドフォン１２のように処理能力の低い機器の場合には、Ｓｏｕｒｃｅ装置１１は、発生する乱数ｘを８ビットにするとともに、演算ｆ（ｘ）をビットシフトなどの簡単な演算方式にする。ヘッドフォンのように処理能力の低い機器すなわちＴｙｐｅ１の場合、一般に、比較的低い処理能力のＣＰＵが搭載されているので、あまり強度の高くＣＰＵの処理負荷の高い認証処理を行なうのには向いていない。

これに対し、通信相手となるＳｉｎｋ装置がパーソナル・コンピュータ（ＰＣ）１３のように、比較的高い処理能力のＣＰＵが搭載されている装置の場合には、上述したような簡単な演算方式では、容易に「なりすまし」が行なわれて、コンテンツを充分にプロテクトすることができない。したがって、Ｓｉｎｋ装置がＴｙｐｅ２の場合には、Ｓｏｕｒｃｅ装置１１は、発生する乱数ｘを６４ビット又は１２８ビットなどの長いものにするとともに、演算ｆ（ｘ）を楕円関数などの

比較的複雑なものを採用する。

なお、認証の演算として、ここでは乱数を入力して演算を行なう例を挙げたが、乱数だけではなく、例えばＳｉｎｋ装置のＢｌｕｅｔｏｏｔｈアドレス(BD_ADDR)など装置固有のデータを用いることにより、認証の強度をさらに向上させることができる。

上述したように通信相手となるＳｉｎｋ装置の用途に応じて認証方式を切り換える場合において、最も重要となるのは、Ｓｉｎｋ装置のタイプの判別方法である。例えば、本発明に係る認証方式には非対応（すなわち、ライセンスでの規制範囲外）のパーソナル・コンピュータが「ヘッドフォンである」となりすまして、不正にストリーム・データを記録してしまうような事態を防止しなければならない。

なお、認証演算による負荷が重たい機器（例えば、ＰＣのように高い演算機能を持つ機器）は基本的にＴｙｐｅ２を採用する。本発明に係る認証方式では、逆にＴｙｐｅ１の対象機器を絞り込む。

Ｓｉｎｋ装置のタイプ（Ｔｙｐｅ１，Ｔｙｐｅ２）の判別方法について、以下に詳解する。

（１）自己申告

Ｓｏｕｒｃｅ機器から"Stream Get Capability"コマンドを受け取ったＳｉｎｋ装置は、本実施形態に係るコンテンツ・プロテクション方式に対応していることをＣＰ－ＴＹＰＥで示す。"Stream Get Capability"のコマンド及びレスポンスに使用されるデータ・フレームの構造を図１１及び図１２にそれぞれ示しておく。

本実施形態に係るコンテンツ・プロテクション方式に対応しているＳｏｕｒｃｅ装置は、Ｓｉｎｋ装置に対して、"Stream Set Configuration"コマンドを送り、本プロテクション方式を適用するようにセットする。"Stream Set Configuration"のコマンド及びレスポンスに使用されるデータ・フレームの構造を図１３に示しておく。

次いで、Ｓｏｕｒｃｅ装置は、"Security Control"コマンドを用いて、Ｓｉｎｋ装置に対してタイプを問い合わせる。"Security Control"のコマンド及びレスポンスに使用されるデータ・フレームの構造を図１４及び図１５にそれぞれ示し

ておく。また、タイプ問い合わせ時のこれらコマンド及びレスポンスにおける"Content Protection Scheme Dependent"フィールドの構成を図１６及び図１７にそれぞれ示しておく。

"Content Protection Scheme Dependent"フィールドのフィールド長は、コマンド・レスポンス種別により可変長とするが、タイプ問い合わせコマンドの場合は1バイトとし、４ビットでコマンド・レスポンスの種別を示すとともに、４ビットでパラメータを示す。また、タイプ問い合わせコマンドでは、レスポンスの際に４ビットでタイプを示す。Ｔｙｐｅ１の場合は"０００１"となり、Ｔｙｐｅ２の場合は"００１０"となる。

（２）Ｔｙｐｅ１の確認

Ｓｉｎｋ装置がＴｙｐｅ２を自己申告した場合には、Ｔｙｐｅ２に適合した方式で認証が行なわれる。また、Ｓｉｎｋ装置がＴｙｐｅ１及びＴｙｐｅ２以外の値を返してきた場合には、そこで認証は失敗とする。また、Ｓｉｎｋ装置がＴｙｐｅ１を自己申告した場合は、さらにその確認のために以下の処理手順を実行する。

（２－１）Ｃｌａｓｓ　ｏｆ　Ｄｅｖｉｃｅ

Ｓｏｕｒｃｅ装置は、Ｉｎｑｕｉｒｙ処理手続の際に、Ｓｉｎｋ装置のＣｌａｓｓ　ｏｆ　Ｄｅｖｉｃｅを入手するので(図７を参照のこと)、ここではＳｉｎｋ装置のＣｌａｓｓ　ｏｆ　Ｄｅｖｉｃｅ情報を基にＳｉｎｋ装置のタイプの確認を行なうことができる。" Bluetooth Assigned Numbers "に規定されているように、各Ｂｌｕｅｔｏｏｔｈ機器は自分が何者であるかを、" Major Device Class "及び"Minor Device Class"で示すようになっている。Ｓｉｎｋ装置の Major Device Class が"Computer"の場合は、このＳｉｎｋ装置はＴｙｐｅ２による認証の対象であり、Ｔｙｐｅ１であることを自己申告したということは「なりすまし」であると解釈する。すなわち、Ｓｉｎｋ装置の Major Device Class が"Computer"の場合は、認証はここで失敗とする。

図１８には、Ｃｌａｓｓ　ｏｆ　Ｄｅｖｉｃｅ情報フィールドのデータ構造を模式的に示している。同図に示すように、当該フィールドの先頭から１２ビット目からの５ビットがMajor Device Classに割り当てられている。また、Bluetooth

Assigned Numbersが規定するMajor Device Classの割り当てを図１９に示しておく。

（２－２）プロファイル

Major Device Class が"Computer"でなくても、高機能な装置であれば、簡単な認証方式であるＴｙｐｅ１の対象とはならない。そこで、Ｓｏｕｒｃｅ装置は、Ｓｉｎｋ装置がオーディオ伝送以外にサポートしているＢｌｕｅｔｏｏｔｈアプリケーション・プロファイルがあるかどうかを調べる。ＳＤＰによりＢｌｕｅｔｏｏｔｈ機器のサポート・プロファイルを知ることができる。

Ｓｉｎｋ装置がＡ２ＤＰ以外のプロファイルをサポートしていない場合には、このＳｉｎｋ装置をＴｙｐｅ１すなわちレンダリング用途としての認証の対象であると認定する。

また、Ｓｉｎｋ装置がこれら以外のプロファイルに対応している場合には、対応しているプロファイルを基に判断する。Ｓｉｎｋ装置が、"Personal Area Network"（ＰＡＮ）、"LAN Access Profile"（ＬＡＮ）、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのいずれかのプロファイルをサポートしている場合には、このＳｉｎｋ装置をＴｙｐｅ２としての認証の対象であると認定して、認証はここで失敗とする。

（３）認証

Ｓｏｕｒｃｅ装置は、Ｓｉｎｋ装置がＴｙｐｅ１又はＴｙｐｅ２のいずれであるかの認証を、"Security Control"コマンドを用いて行う。認証時における該コマンドのコマンド及びレスポンスにおける"Content Protection Scheme Dependent"フィールドの構成を図２０及び図２１にそれぞれ示しておく。

図２２及び図２３には、Ｓｏｕｒｃｅ装置１１がＳｉｎｋ装置１２のタイプ判別を行うことにより認証を行なうための処理手順をフローチャートの形式で示している。以下、これらのフローチャートに従って、本実施形態に係る認証処理について説明する。

Ｓｏｕｒｃｅ装置１１は、Ｓｉｎｋ装置１２とはＢｌｕｅｔｏｏｔｈベースバンド層において接続が確立され、呼び出し（Ｐａｇｅ）によりＳｉｎｋ装置の装置種別（Class of Device）を取得しているとともに、ＳＤＰプロトコルによりＳ

ｉｎｋ装置がサポートしているサービス（対応しているプロトコルやプロファイル）を取得しているものとする。

Ｓｏｕｒｃｅ装置１１は、ＡＶＤＴＰプロトコルに従い、Ｓｉｎｋ装置１２に"Stream Get Capability"コマンドを送信して、そのレスポンスのＣＰ＿ＴＹＰＥが示す値を基に、Ｓｉｎｋ装置１２が本発明に係るコンテンツ・プロテクション方式に対応するか否かを判別する（ステップＳ１）。

ＣＰ＿ＴＹＰＥを基に、Ｓｉｎｋ装置１２が本プロテクション方式に対応していない場合には、本処理ルーチン全体を終了する。

一方、Ｓｉｎｋ装置１２が本プロテクション方式に対応していると判断された場合には、Ｓｏｕｒｃｅ装置１１は、Ｓｉｎｋ装置１２に対して、"Stream Set Configuration"コマンドを送り、本プロテクション方式を適用するようにセットする（ステップＳ２）。ここまでの手続は、ＡＶＤＴＰプロトコルに従って行なうことができる。

次いで、Ｓｏｕｒｃｅ装置１１のアプリケーション層は、"Security Control"コマンドを用いて、Ｓｉｎｋ装置１２に対してタイプを問い合わせる（ステップＳ３）。ここで行なわれるタイプ問い合わせすなわち認証処理は、Ｓｉｎｋ装置１２からの自己申告に基づく。ここで言うＳｉｎｋ装置１２のタイプは、該装置がヘッドフォンなどの処理能力の低いか（Ｔｙｐｅ１）、又は、パーソナル・コンピュータ（ＰＣ）などの処理能力の高い機器か（Ｔｙｐｅ２）で区分される。

Ｓｉｎｋ装置１２がＴｙｐｅ１以外の値を返してきた場合には(ステップＳ４)、さらに、Ｓｉｎｋ装置１２がＴｙｐｅ２を自己申告したか否かを判別する（ステップＳ５）。

Ｓｉｎｋ装置１２がＴｙｐｅ２を自己申告した場合には（ステップＳ５）、本処理ルーチン全体を終了して、以後、Ｔｙｐｅ２に適合した方式で認証が行われる（ステップＳ６）。Ｔｙｐｅ２に適合した認証方式とは、例えば、図１０に示す認証メカニズムにおいて、Ｓｏｕｒｃｅ装置１１が、発生する乱数ｘを６４ビット又は１２８ビットなどの長いものにするとともに、演算ｆ（ｘ）を楕円関数などの比較的複雑なものを採用することによって実現される。

Ｔｙｐｅ２に適合した認証に成功した場合には（ステップＳ７）、本処理ルーチ

ンは成功裏に終了する。これに対し、Ｔｙｐｅ２認証に失敗した場合には、認証は失敗として、本処理ルーチン全体を終了する。また、Ｓｉｎｋ装置１２がＴｙｐｅ２以外の値を返してきた場合には（ステップＳ５）、そこで認証は失敗として、本処理ルーチン全体を終了する。

また、Ｓｉｎｋ装置１２がＴｙｐｅ１を自己申告した場合には（ステップＳ４）、さらに、Ｓｉｎｋ装置１２の装置種別（Class of Device）を確認する（ステップＳ８）。Ｓｉｎｋ装置１２のClass of Deviceは、Ｎａｍｅ　Ｄｉｓｃｏｖｅｒｙ処理手続時に行われる呼び出し（Ｐａｇｅ）によって既に取得されている。

Ｓｉｎｋ装置１２のMajor Device Classが"Computer"の場合は、このＳｉｎｋ装置１２はＴｙｐｅ２による認証の対象であり、Ｔｙｐｅ１であることを自己申告したということは「なりすまし」であると解釈する（ステップＳ８）。すなわち、Ｓｉｎｋ装置のMajor Device Classが"Computer"の場合は、認証はここで失敗とする。

他方、Major Device Classが"Computer"でなくても、高機能な装置であれば、簡単な認証方式であるＴｙｐｅ１の対象とはならない。そこで、Ｓｏｕｒｃｅ装置１１は、Ｓｉｎｋ装置１２がオーディオ伝送以外にサポートしているＢｌｕｅｔｏｏｔｈアプリケーション・プロファイルがあるかどうかを調べる（ステップＳ１２）。

Ｓｉｎｋ装置１２がＡ２ＤＰ以外のプロファイルをサポートしていない場合には、このＳｉｎｋ装置１２をＴｙｐｅ１の認証の対象であると認定して、Ｔｙｐｅ１に適合した方式で認証を行う（ステップＳ１０）。Ｔｙｐｅ１に適合した認証方式とは、例えば、図１０に示す認証メカニズムにおいて、Ｓｏｕｒｃｅ装置が、発生する乱数ｘを８ビットにするとともに、演算ｆ（ｘ）にビットシフトなどの比較的簡単なものを採用することによって実現される。Ｔｙｐｅ１に適合した認証に成功した場合には（ステップＳ１１）、本処理ルーチンは成功裏に終了する。これに対し、Ｔｙｐｅ１認証に失敗した場合には、認証は失敗として、本処理ルーチン全体を終了する。

また、Ｓｉｎｋ装置１２がＡ２ＤＰ以外のプロファイルをサポートしている場合には、さらに、Ｓｉｎｋ装置１２が、"Personal Area Network"（ＰＡＮ）、"LAN

Access Profile" (ＬＡＮ)、Ｏｂｊｅｃｔ　Ｐｕｓｈ　Ｐｒｏｆｉｌｅ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｆｉｌｅのいずれかをサポートしているか否かを判別する（ステップＳ８）。

Ｓｉｎｋ装置１２が、"Personal Area Network" (ＰＡＮ)、"LAN Access Profile" (ＬＡＮ)、Ｏｂｊｅｃｔ　Ｐｕｓｈ　Ｐｒｏｆｉｌｅ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｆｉｌｅのいずれかをサポートしている場合には（ステップＳ９）、このＳｉｎｋ装置１２をＴｙｐｅ２の認証の対象であると認定して、認証はここで失敗とする。

他方、Ｓｉｎｋ装置１２が、"Personal Area Network" (ＰＡＮ)、"LAN Access Profile" (ＬＡＮ)、Ｏｂｊｅｃｔ　Ｐｕｓｈ　Ｐｒｏｆｉｌｅ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｆｉｌｅのいずれもサポートしていない場合には（ステップＳ９）、このＳｉｎｋ装置１２をＴｙｐｅ１の認証の対象であると認定して、Ｔｙｐｅ１に適合した方式で認証を行い、本処理ルーチン全体を終了する（同上）。

なお、ＳＤＰのBluetooth Profile Descriptor Listにはその機器が対応しているプロファイルが列挙されている。そして、Bluetooth Assigned Numbersで各プロファイルにＵＵＩＤが割り振られている。図２４には、ＵＵＩＤの例（抜粋）を示している。上述したステップＳ９及びＳ１２では、このBluetooth Profile Descriptor ListのＵＵＩＤを参照することによって、機器がサポートしているプロファイルを判断することができる。

追補

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

本明細書では、本発明をＢｌｕｅｔｏｏｔｈワイヤレス・ネットワークに適用した場合を例にとって説明してきたが、本発明の要旨は必ずしもこれに限定されるものではなく、同様の機器情報、サービス情報を取り扱う他の有線及び無線伝送システムにおいても本発明を適用することができる。

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載

内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

[産業上の利用可能性]

本発明によれば、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

また、本発明によれば、Ｂｌｕｅｔｏｏｔｈのように１台のマスタ（ｍａｓｔｅｒ）機器と複数台のスレーブ（ｓｌａｖｅ）機器によって構成されるピコネット（ｐｉｃｏｎｅｔ）内において機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

また、本発明によれば、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらＢｌｕｅｔｏｏｔｈ機器間で伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

本発明によれば、オーディオ・データなどプロテクションを施す必要があるデータをＢｌｕｅｔｏｏｔｈ接続により伝送する場合、通信相手となる機器の処理能力に応じて認証の難易度を切り替えることができ、Ｂｌｕｅｔｏｏｔｈによるセキュアなオーディオ伝送を実現することができる。したがって、ヘッドフォンのような低い処理能力の機器であっても、ＳＤＭＩに準拠したＢｌｕｅｔｏｏｔｈ通信を行なうことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、充分なハッキング対策を施すことができる。

請求の範囲

1．所定の無線セル内でデータ・ストリームを送信するＳｏｕｒｃｅ装置とデータ・ストリームを受信するＳｉｎｋ装置とからなる無線通信システムであって、

前記Ｓｉｎｋ装置の処理能力を判別する判別手段と、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御手段と、

を具備することを特徴とする無線通信システム。

2．前記判別手段は、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプの装置か、又は、処理能力の高い第２のタイプの装置かを判別する、

ことを特徴とする請求項１に記載の無線通信システム。

3．前記認証制御手段は、前記Ｓｉｎｋ装置が第１のタイプの場合は比較的簡単な認証方式を採用し、前記Ｓｉｎｋ装置が第２のタイプの場合は比較的複雑な認証方式を採用する、

ことを特徴とする請求項２に記載の無線通信システム。

4．前記判別手段は、前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

5．前記判別手段は、前記Ｓｉｎｋ装置の種別を基に前記Ｓｉｎｋ装置の処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

6．前記判別手段は、前記Ｓｉｎｋ装置がサポートするサービスを基に前記Ｓｉｎｋ装置の処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

7．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、

前記判別手段は、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義されるStream Get Capabilityコマンドを用いて前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

8．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、

前記判別手段は、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義されるSecurity Controlコマンドを用いて前記Ｓｉｎｋ装置に処理能力を問い合わせる、

ことを特徴とする請求項１に記載の無線通信システム。

9．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、

前記判別手段は、問い合わせ（Ｉｎｑｕｉｒｙ）処理手続の際に入手したClass of Device情報を基に、前記Ｓｉｎｋ装置の処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

１０．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、

前記判別手段は、サービス・ディスカバリ（Service Discovery）によって取得された前記Ｓｉｎｋ装置が対応するサービス（プロトコル又はプロファイル）によってその処理能力を判別する、

ことを特徴とする請求項１に記載の無線通信システム。

１１．前記判別手段は、前記Ｓｉｎｋ装置がＡ２ＤＰ（Bluetooth Advanced Audio

Distribution Profile) にのみ対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプであると判断する、
ことを特徴とする請求項１０に記載の無線通信システム。

１２．前記判別手段は、前記Ｓｉｎｋ装置がＰＡＮ (Personal Area Network)、ＬＡＮ (LAN Access Profile)、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのうち少なくとも１つのプロファイルに対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプではないと判断する、
ことを特徴とする請求項１０に記載の無線通信システム。

１３．所定の無線セル内でＳｉｎｋ装置に対してデータ・ストリームを送信する無線通信制御装置であって、
前記Ｓｉｎｋ装置の処理能力を判別する判別手段と、
該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御手段と、
を具備することを特徴とする無線通信制御装置。

１４．前記判別手段は、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプの装置か、又は、処理能力の高い第２のタイプの装置かを判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

１５．前記認証制御手段は、前記Ｓｉｎｋ装置が第１のタイプの場合は比較的簡単な認証方式を採用し、前記Ｓｉｎｋ装置が第２のタイプの場合は比較的複雑な認証方式を採用する、
ことを特徴とする請求項１４に記載の無線通信制御装置。

１６．前記判別手段は、前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

１７．前記判別手段は、前記Ｓｉｎｋ装置の種別を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

１８．前記判別手段は、前記Ｓｉｎｋ装置がサポートするサービスを基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

１９．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別手段は、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義されるStream Get Capabilityコマンドを用いて前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

２０．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別手段は、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義されるSecurity Controlコマンドを用いて前記Ｓｉｎｋ装置に処理能力を問い合わせる、
ことを特徴とする請求項１３に記載の無線通信制御装置。

２１．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別手段は、問い合わせ（Ｉｎｑｕｉｒｙ）処理手続の際に入手したClass of Device情報を基に、前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項１３に記載の無線通信制御装置。

２２．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、

前記判別手段は、サービス・ディスカバリ（Service Discovery）によって取得された前記Ｓｉｎｋ装置が対応するサービス（プロトコル又はプロファイル）によってその処理能力を判別する、

ことを特徴とする請求項１３に記載の無線通信制御装置。

２３．前記判別手段は、前記Ｓｉｎｋ装置がＡ２ＤＰ（Bluetooth Advanced Audio Distribution Profile）にのみ対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプであると判断する、

ことを特徴とする請求項２２に記載の無線通信制御装置。

２４．前記判別手段は、前記Ｓｉｎｋ装置がＰＡＮ（Personal Area Network）、ＬＡＮ（LAN Access Profile）、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのうち少なくとも１つのプロファイルに対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプではないと判断する、

ことを特徴とする請求項２２に記載の無線通信制御装置。

２５．所定の無線セル内でＳｉｎｋ装置に対するデータ・ストリームの送信を制御する無線通信制御方法であって、

前記Ｓｉｎｋ装置の処理能力を判別する判別ステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とする無線通信制御方法。

２６．前記判別ステップでは、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプの装置か、又は、処理能力の高い第２のタイプの装置かを判別する、

ことを特徴とする請求項２５に記載の無線通信制御方法。

２７．前記認証制御ステップでは、前記Ｓｉｎｋ装置が第１のタイプの場合は比較的簡単な認証方式を採用し、前記Ｓｉｎｋ装置が第２のタイプの場合は比較的複雑な認証方式を採用する、
ことを特徴とする請求項２６に記載の無線通信制御方法。

２８．前記判別ステップでは、前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

２９．前記判別ステップでは、前記Ｓｉｎｋ装置の種別を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３０．前記判別ステップでは、前記Ｓｉｎｋ装置がサポートするサービスを基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３１．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別ステップでは、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義される Stream Get Capability コマンドを用いて前記Ｓｉｎｋ装置からの自己申告を基に前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３２．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別ステップでは、オーディオ伝送用のＡＶＤＴＰ（Audio Video Distribution Transport Protocol）プロトコルで定義される Security Control

コマンドを用いて前記Ｓｉｎｋ装置に処理能力を問い合わせる、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３３．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別ステップでは、問い合わせ（Ｉｎｑｕｉｒｙ）処理手続の際に入手したClass of Device情報を基に、前記Ｓｉｎｋ装置の処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３４．前記無線セルは、Ｂｌｕｅｔｏｏｔｈワイヤレス・ネットワークにより構築され、
前記判別ステップでは、サービス・ディスカバリ（Service Discovery）によって取得された前記Ｓｉｎｋ装置が対応するサービス（プロトコル又はプロファイル）によってその処理能力を判別する、
ことを特徴とする請求項２５に記載の無線通信制御方法。

３５．前記判別ステップでは、前記Ｓｉｎｋ装置がＡ２ＤＰ（Bluetooth Advanced Audio Distribution Profile）にのみ対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプであると判断する、
ことを特徴とする請求項３４に記載の無線通信制御方法。

３６．前記判別ステップでは、前記Ｓｉｎｋ装置がＰＡＮ(Personal Area Network)、ＬＡＮ（LAN Access Profile)、Ｏｂｊｅｃｔ　Ｐｕｓｈ、又は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒのうち少なくとも１つのプロファイルに対応している場合には、前記Ｓｉｎｋ装置が処理能力の低い第１のタイプではないと判断する、
ことを特徴とする請求項３４に記載の無線通信制御方法。

３７．所定の無線セル内でＳｉｎｋ装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフト

ウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記Ｓｉｎｋ装置の処理能力を判別する判別ステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とする記憶媒体。

３８．所定の無線セル内でＳｉｎｋ装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・プログラムであって、

前記Ｓｉｎｋ装置の処理能力を判別する判別ステップと、

該判別された前記Ｓｉｎｋ装置の処理能力に応じて、前記Ｓｏｕｒｃｅ装置との前記Ｓｉｎｋ装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とするコンピュータ・プログラム。

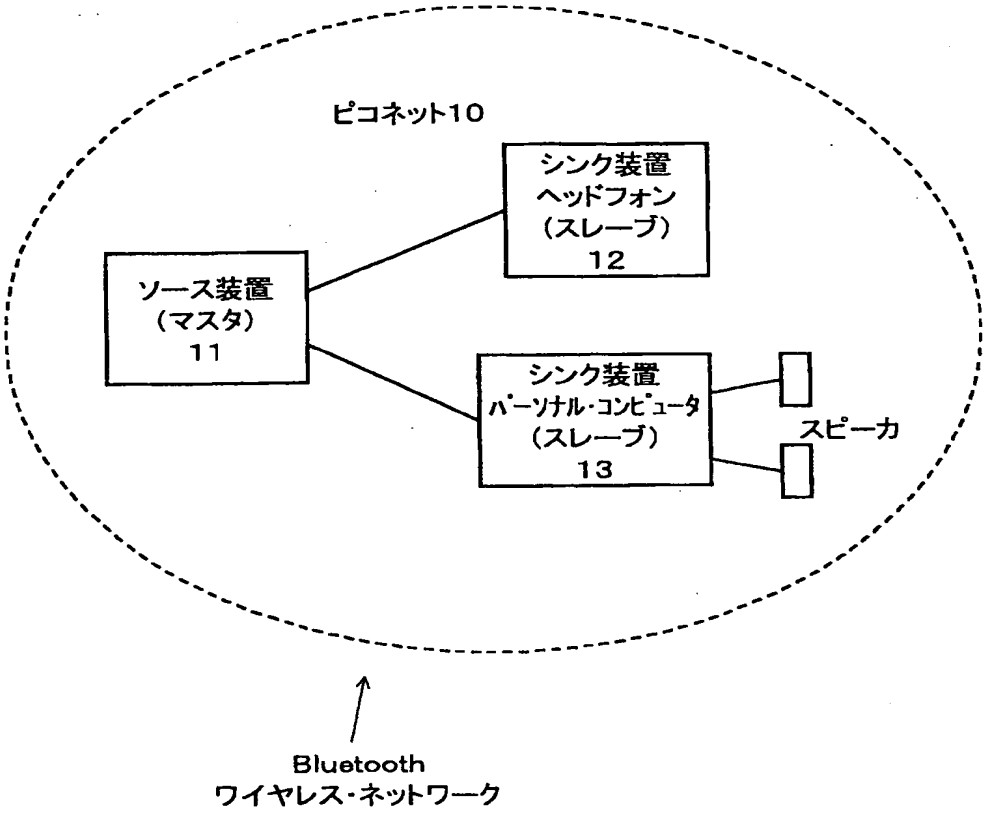

ピコネット10
シンク装置
ヘッドフォン
(スレーブ)
12
ソース装置
(マスタ)
11
シンク装置
パーソナル・コンピュータ
(スレーブ)
13
スピーカ
Bluetooth
ワイヤレス・ネットワーク

図1

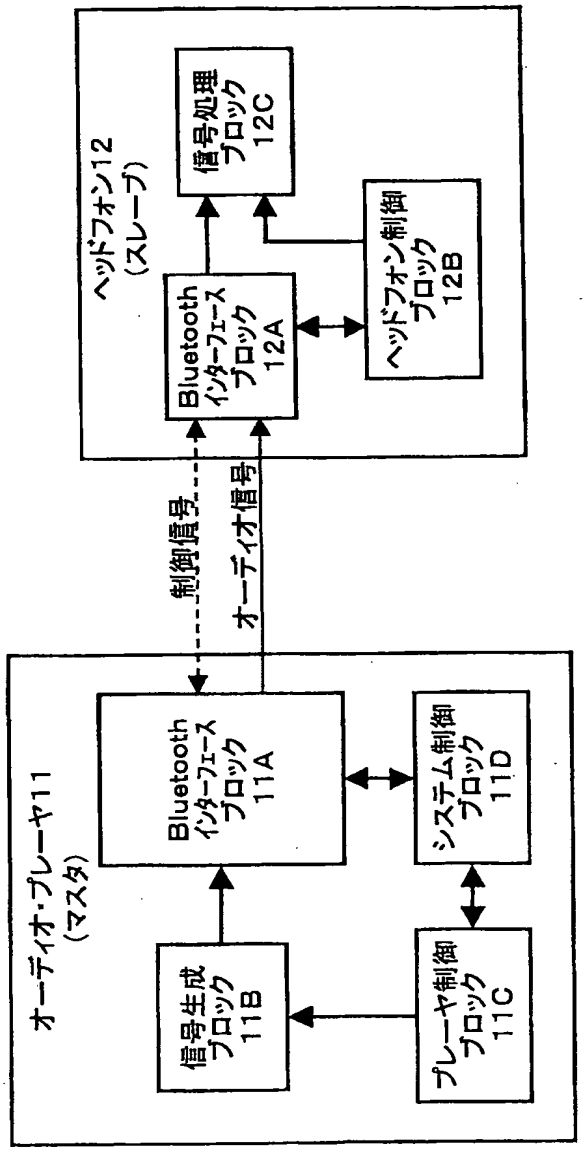

ヘッドフォン12
(スレーブ)
信号処理
ブロック
12C
ヘッドフォン制御
ブロック
12B
Bluetooth
インターフェース
ブロック
12A
制御信号
オーディオ信号
オーディオ・プレーヤ11
(マスタ)
Bluetooth
インターフェース
ブロック
11A
システム制御
ブロック
11D
信号生成
ブロック
11B
プレーヤ制御
ブロック
11C

図2

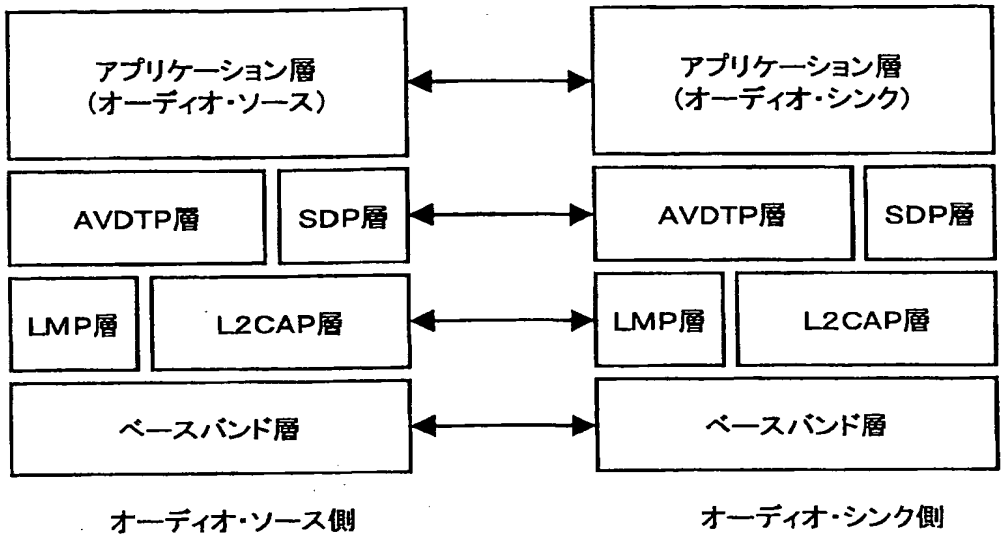

アプリケーション層
(オーディオ・ソース)
アプリケーション層
(オーディオ・シンク)
AVDTP層
SDP層
AVDTP層
SDP層
LMP層
L2CAP層
LMP層
L2CAP層
ベースバンド層
ベースバンド層
オーディオ・ソース側
オーディオ・シンク側

図3

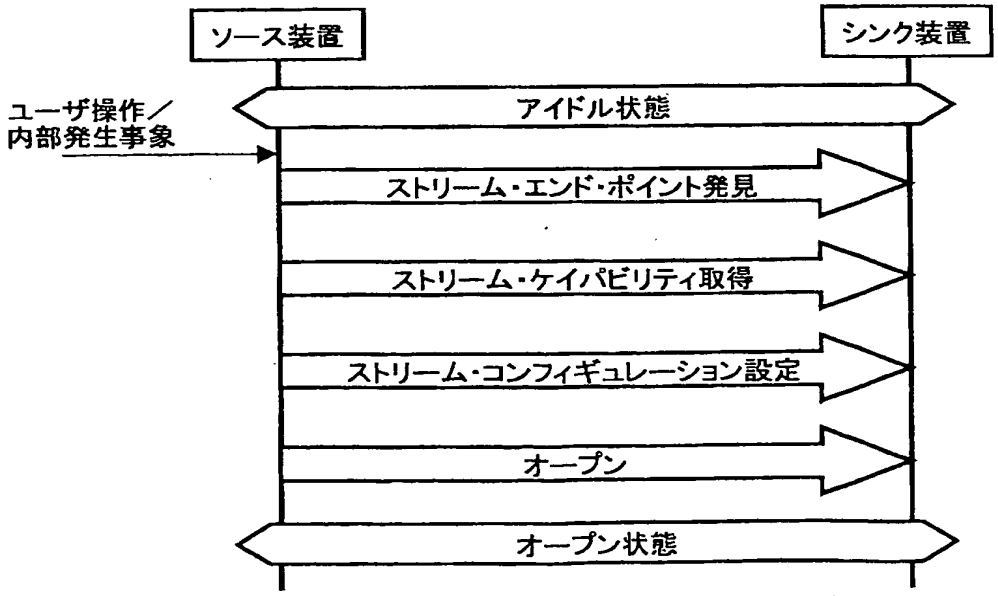

ソース装置
シンク装置
ユーザ操作／
内部発生事象
アイドル状態
ストリーム・エンド・ポイント発見
ストリーム・ケイパビリティ取得
ストリーム・コンフィギュレーション設定
オープン
オープン状態

図4

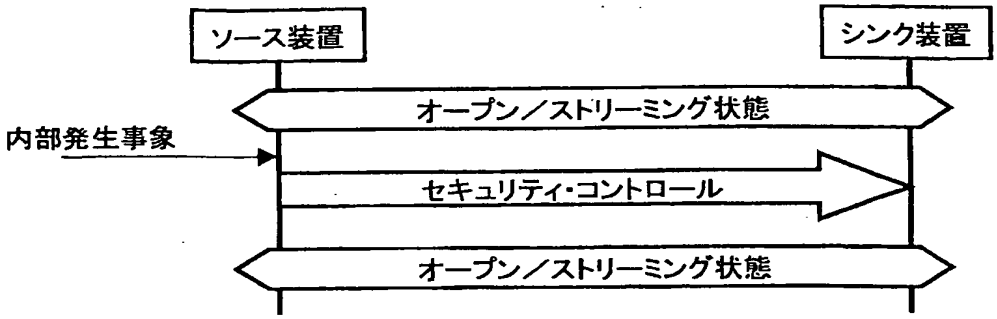

ソース装置
シンク装置
オープン／ストリーミング状態
内部発生事象
セキュリティ・コントロール
オープン／ストリーミング状態

図5

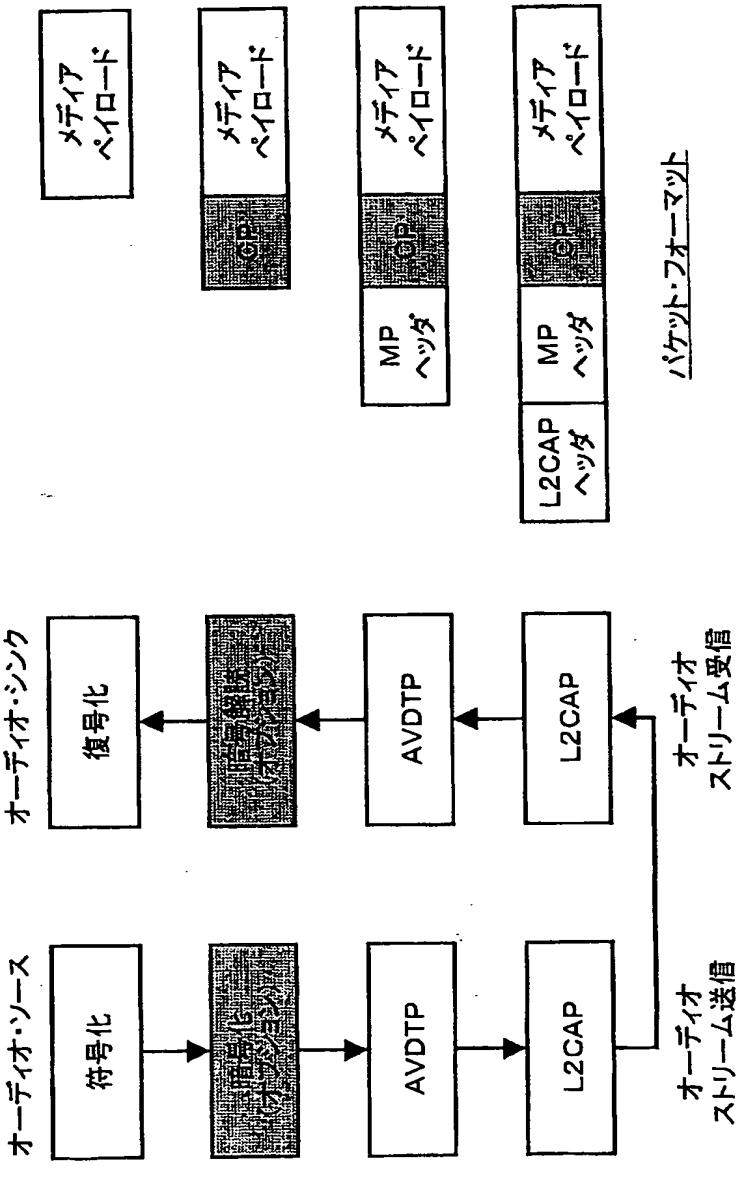

メディア ペイロード
メディア ペイロード
OP
メディア ペイロード
MP ヘッダ
OP
メディア ペイロード
L2CAP ヘッダ
MP ヘッダ
OP
パケット・フォーマット
オーディオ・シンク
復号化
暗号解読 (オプション)
AVDTP
L2CAP
オーディオ ストリーム受信
オーディオ・ソース
符号化
暗号化 (オプション)
AVDTP
L2CAP
オーディオ ストリーム送信

図6

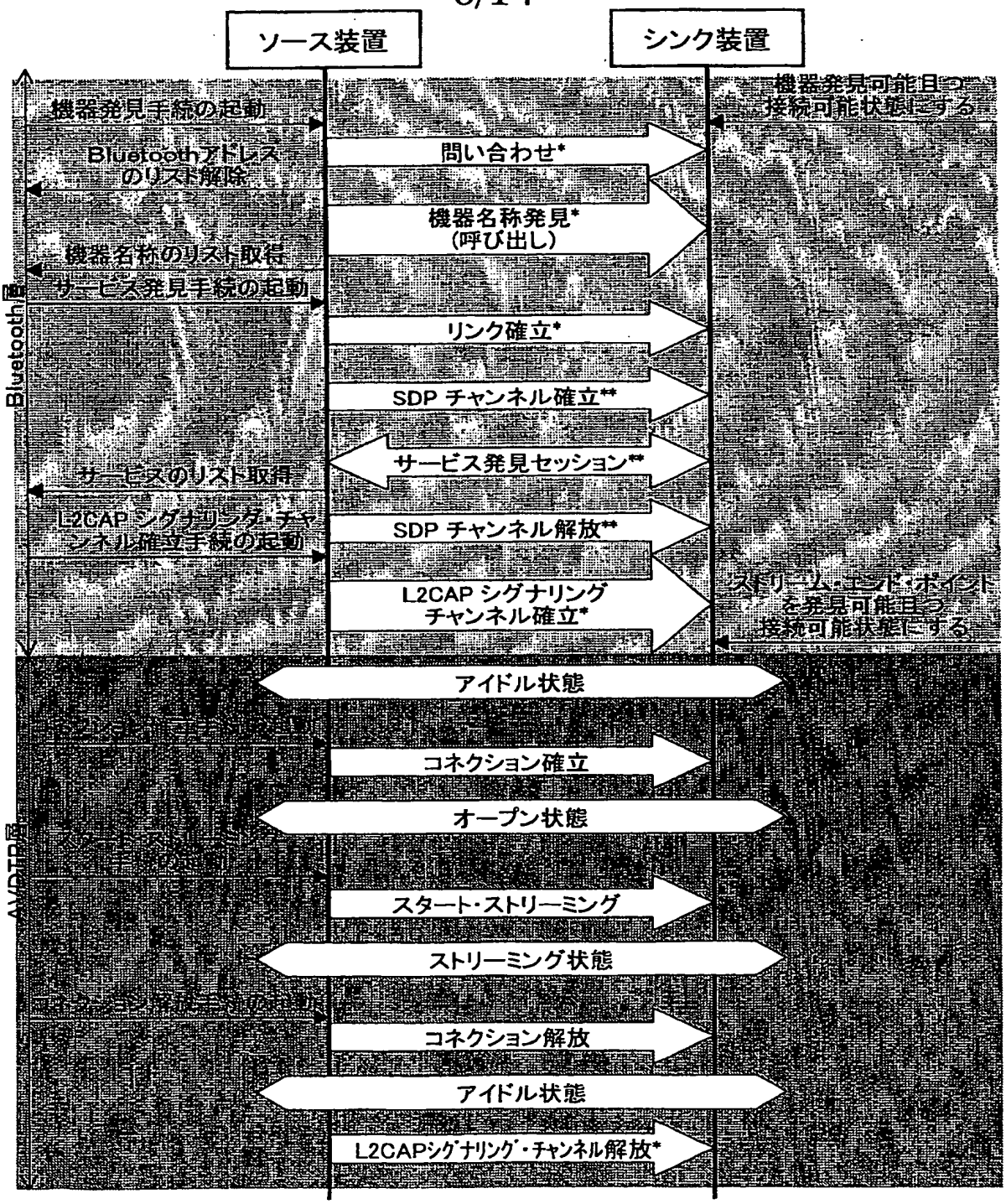

ソース装置
シンク装置
機器発見可能且つ接続可能状態にする
機器発見手続の起動
問い合わせ*
Bluetoothアドレスのリスト解除
機器名称発見*
(呼び出し)
機器名称のリスト取得
サービス発見手続の起動
リンク確立*
SDP チャンネル確立**
サービス発見セッション**
サービスのリスト取得
SDP チャンネル解放**
L2CAP シグナリング・チャンネル確立手続の起動
L2CAP シグナリング
チャンネル確立*
ストリーム・エンド・ポイントを発見可能且つ接続可能状態にする
Bluetooth層
アイドル状態
コネクション確立
オープン状態
AVDTP層
スタート・ストリーミング
ストリーミング状態
コネクション解放
アイドル状態
L2CAPシグナリング・チャンネル解放*

図7

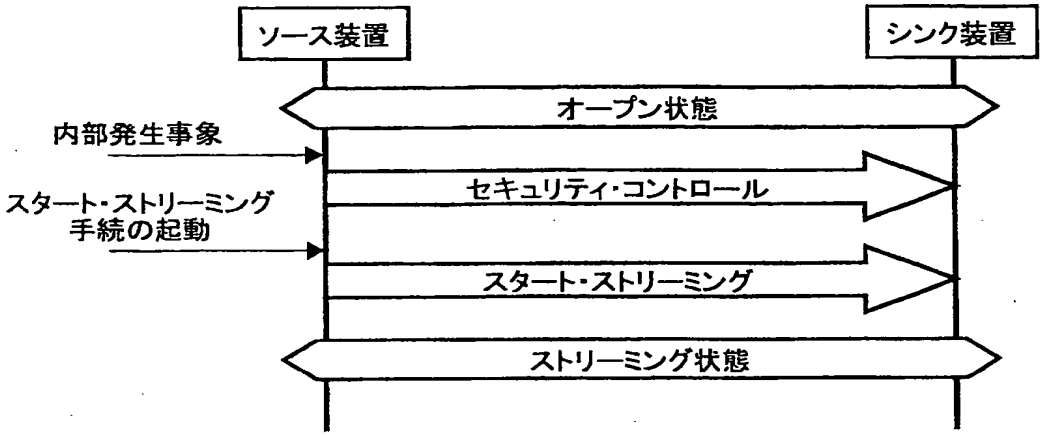

ソース装置
シンク装置
オープン状態
内部発生事象
セキュリティ・コントロール
スタート・ストリーミング
手続の起動
スタート・ストリーミング
ストリーミング状態

図8

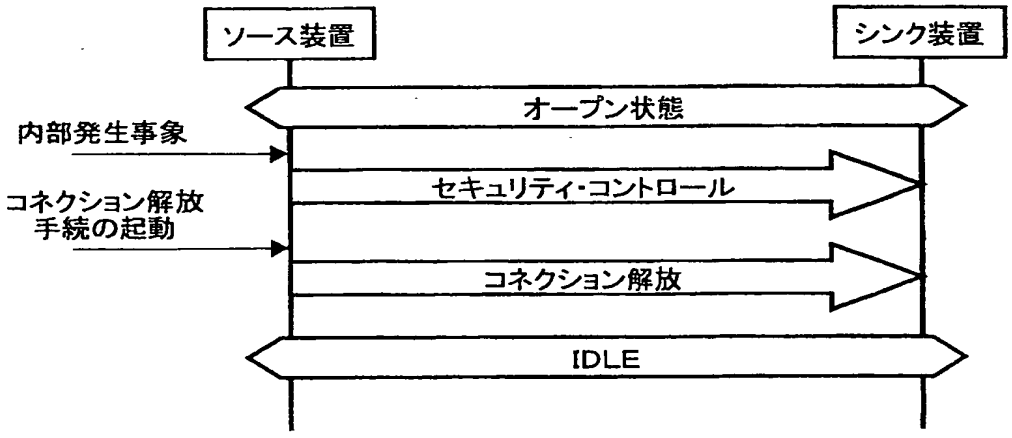

ソース装置
シンク装置
オープン状態
内部発生事象
セキュリティ・コントロール
コネクション解放
手続の起動
コネクション解放
IDLE

図9

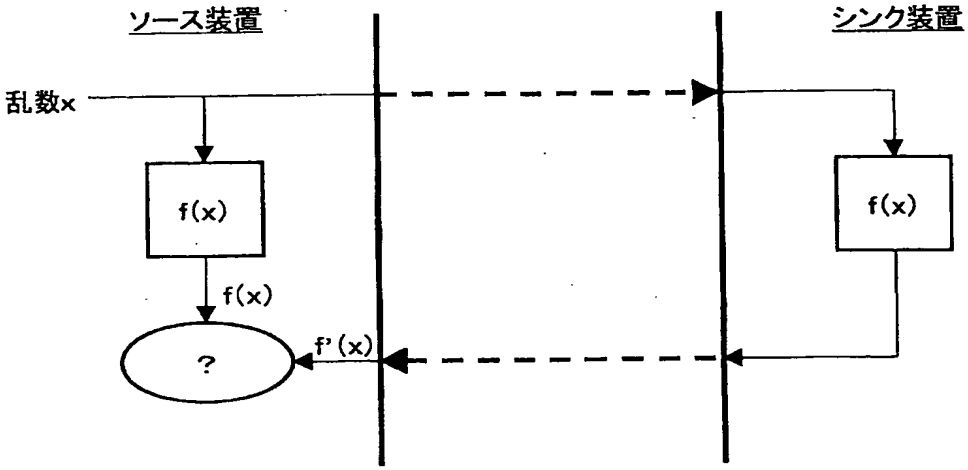


図10

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
0	0	AVDTP_GET_CAPABILITIES						1
ストリーム・エンドポイント識別子(SEID)						1	1	2

図11

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
1	0	AVDTP_GET_CAPABILITIES						1
ストリーム・エンド・ポイント識別子(SEID)						使用中	1	2
サービス・ケイパビリティ								3

図12

7	6	5	4	3	2	1	0	Octed
サービス・カテゴリ=コンテント・プロテクション								0
Length Of Service Capabilities(LOSC)=0x02								1
CP_TYPE_LSB								2
CP_TYPE_MSB								3

図13

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
0	0	AVDTP_SECURITY_CONTROL						1
ストリーム・エンド・ポイント識別子(SEID)						1	1	2
Content Protection Scheme Dependent								⋮

図14

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
1	0	AVDTP_SECURITY_CONTROL						1
ストリーム・エンド・ポイント識別子(SEID)						1	1	2
Content Protection Scheme Dependent								3

図15

コマンド種別:タイプ問い合わせ	0 0 0 0

図16

レスポンス種別:タイプ	値(0~15)

図17

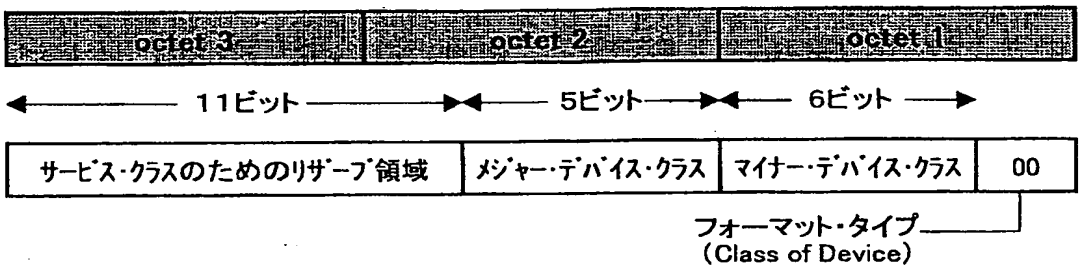


図18

12 11 10 9 8	メジャー・デバイス・クラス
0 0 0 0 0	その他
0 0 0 0 1	コンピュータ(デスクトップ、ノートブック、PDA、オルガナイザ)
0 0 0 1 0	電話(セルラ、コードレス、公衆電話、モデム、...)
0 0 0 1 1	LAN/ネットワークのアクセス・ポイント
0 0 1 0 0	音響/映像(ヘッドセット、スピーカ、ステレオ、ビデオ・ディスプレイ、VCR)
0 0 1 0 1	周辺機器(マウス、ジョイスティック、キーボード)
0 0 1 1 0	画像処理(印刷,スキャナ、カメラ、ディスプレイ、...)
1 1 1 1 1	分類されない特定のデバイス・コード
X X X X X	予約された他のすべての値

図19

コマンド種別：認証	0	0	0	0
x				

図20

レスポンス種別：認証	0	0	0	0
f(x)				

図21

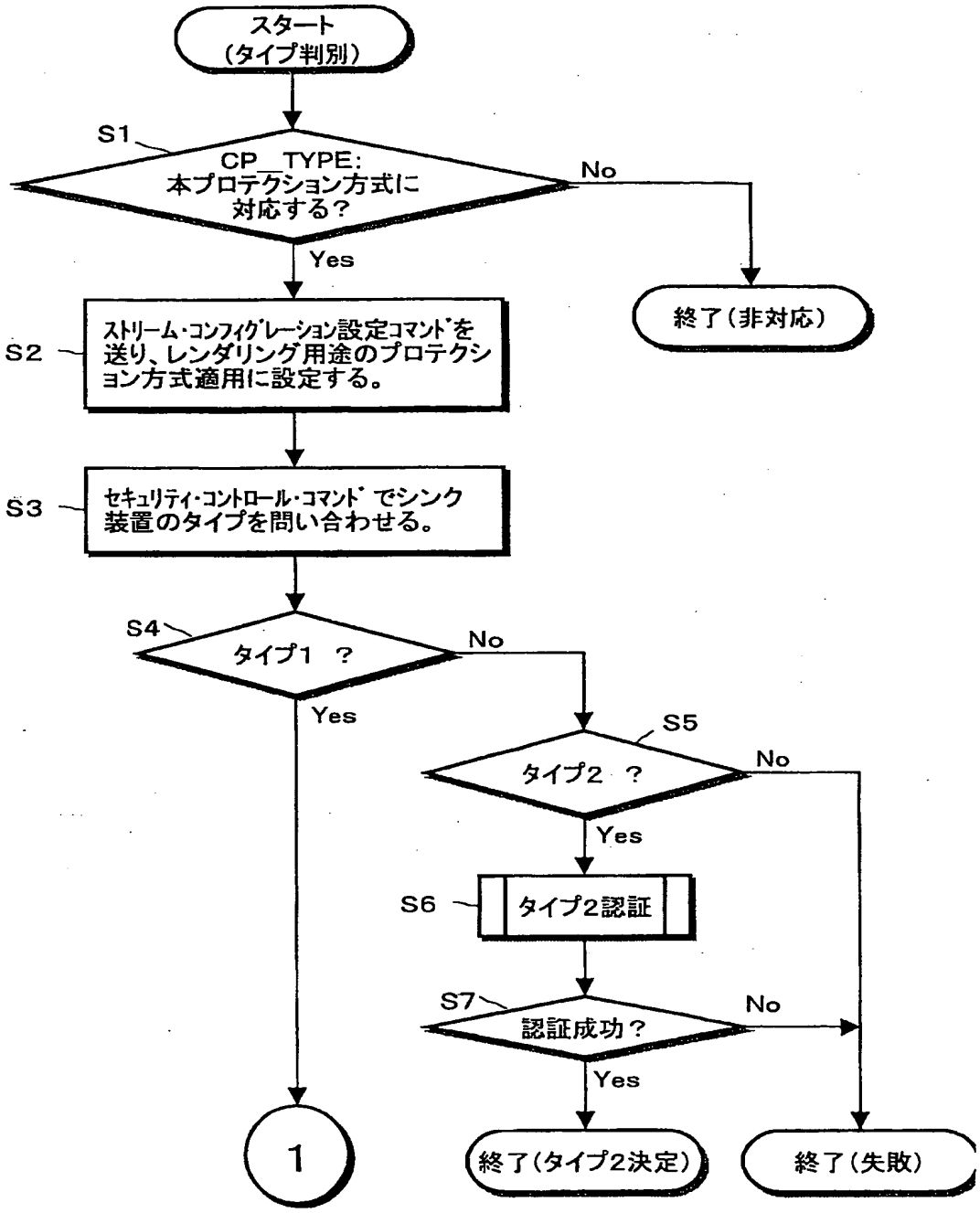

スタート
(タイプ判別)
S1
CP_TYPE:
本プロテクション方式に
対応する?
No
Yes
終了(非対応)
S2
ストリーム・コンフィグレーション設定コマンドを
送り、レンダリング用途のプロテクシ
ョン方式適用に設定する。
S3
セキュリティ・コントロール・コマンド でシンク
装置のタイプを問い合わせる。
S4
タイプ1 ?
No
Yes
S5
タイプ2 ?
No
Yes
S6
タイプ2認証
S7
認証成功?
No
Yes
1
終了(タイプ2決定)
終了(失敗)

図22

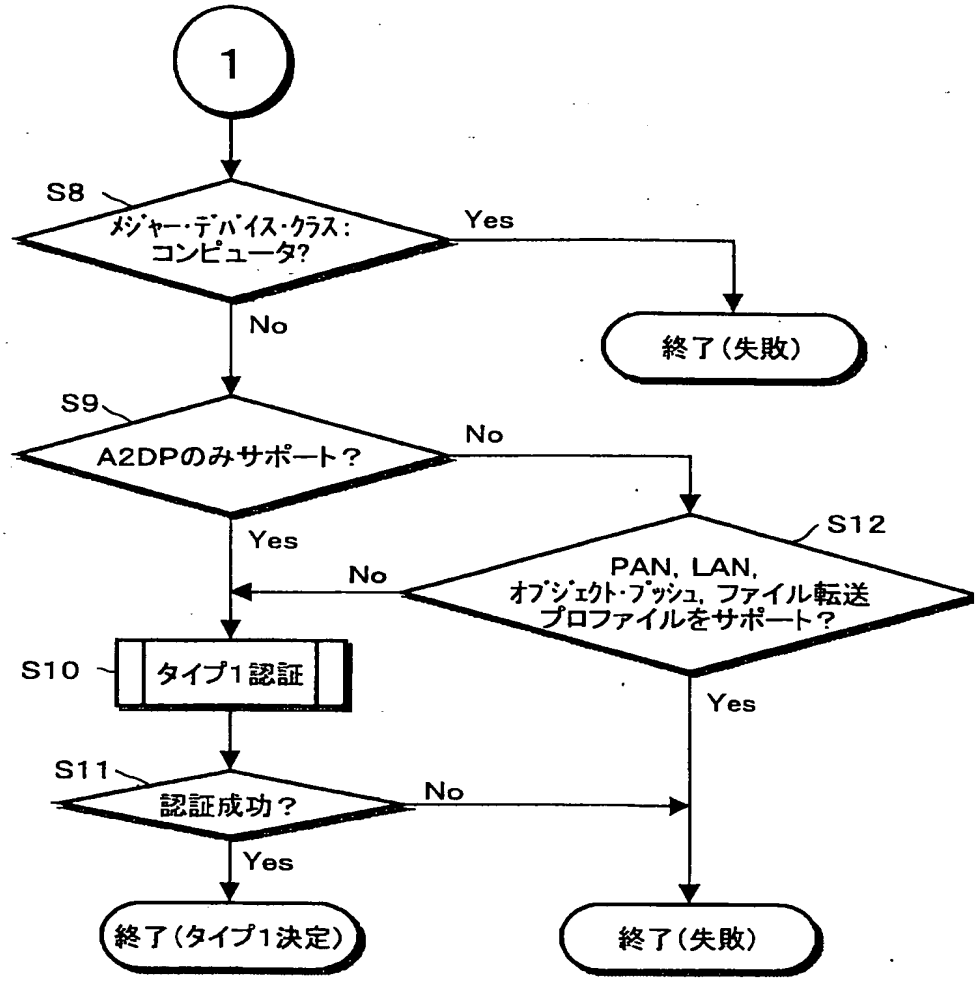

1
S8
メジャー・デバイス・クラス：
コンピュータ?
Yes
終了（失敗）
No
S9
A2DPのみサポート？
No
Yes
S12
PAN, LAN,
オブジェクト・プッシュ, ファイル転送
プロファイルをサポート？
No
Yes
S10
タイプ1認証
S11
認証成功？
No
Yes
終了（タイプ1決定）
終了（失敗）

図23

Profile Name	UUID
シリアル・ポート	0x1101
LAN アクセス	0x1102
ﾀﾞｲﾔﾙｱｯﾌﾟ・ﾈｯﾄﾜｰｷﾝｸﾞ	0x1103
オブジェクト・プッシュ	0x1105
ファイル・トランスファー	0x1106
ヘッドセット	0x1108
ｱﾄﾞﾊﾞﾝｽﾄ・ｵｰﾃﾞｨｵ ﾃｨｽﾄﾘﾋﾞｭｰｼｮﾝ	0x110D
A/V リモート・コントロール	0x110F
PAN	0x1115

図24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07714

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/28, H04L9/00-9/04, H04K1/00-3/00, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1940-2002
Kokai Jitsuyo Shinan Koho 1971-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2000-59323 A (Matsushita Electric Industrial Co., Ltd.), 25 February, 2000 (25.02.00), Full text & WO 99/41910 A1 & EP 977436 A & CN 1263669 T	1-3,13-15, 25-27,37, 38 4-12,16-24, 28-36
Y A	JP 6-261033 A (Nippon Telegraph And Telephone Corp.), 16 September, 1994 (16.09.94), Full text (Family: none)	1-3,13-15, 25-27,37, 38 4-12,16-24, 28-36

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October, 2002 (25.10.02)	12 November, 2002 (12.11.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07714

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-297638 A (Nippon Telegraph And Telephone Corp.), 12 November, 1996 (12.11.96),	1-3,13-15, 25-27,37, 38
A	Full text (Family: none)	4-12,16-24, 28-36
P,A	JP 2001-312472 A (Toshiba Corp.), 09 November, 2001 (09.11.01), Full text (Family: none)	1-38

国際調査報告

国際出願番号 PCT／JP02／07714

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl' H04L12／28

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl' H04L12／28
Int. Cl' H04L9／00－9／04
Int. Cl' H04K1／00－3／00
Int. Cl' G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1940－2002
日本国公開実用新案公報 1971－2002

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2000－59323 A（松下電器産業株式会社）2000.02.25, 全文 & WO99／41910 A1 & EP 977436 A & CN 1263669 T	1－3, 13－15, 25－27, 37, 38
A		4－12, 16－24, 28－36

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
25. 10. 02	12.11.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	8523
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	宮島郁美		
	電話番号 03－3581－1101 内線 3595		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０７７１４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　６－２６１０３３　Ａ（日本電信電話株式会社）１９９４．０９．１６，全文（ファミリーなし）	１－３，１３－１５，２５－２７，３７，３８
Ａ		４－１２，１６－２４，２８－３６
Ｙ	ＪＰ　８－２９７６３８　Ａ（日本電信電話株式会社）１９９６．１１．１２，全文（ファミリーなし）	１－３，１３－１５，２５－２７，３７，３８
Ａ		４－１２，１６－２４，２８－３６
ＰＡ	ＪＰ　２００１－３１２４７２　Ａ（株式会社東芝）２００１．１１．０９，全文（ファミリーなし）	１－３８